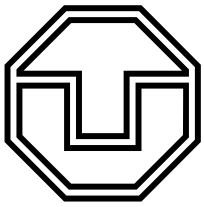

TECHNISCHE UNIVERSITÄT DRESDEN

Department of Mathematics
Bachelor's Thesis (B.Sc.)

Complete Arcs in Projective Spaces, the MDS Main Conjecture and Related Problems

Author:
Jakob Schneider
(* January 26, 1994, in Peine, Germany)

Supervisor:
Prof. Dr. Ulrich Brehm
(Institute of Geometry)

August 8, 2014
(date of submission)

To my grandma.
My thoughts and prayers are with you.

Statutory Declaration

I declare on oath that I completed this work on my own and that information which has been directly or indirectly taken from other sources has been noted as such. Neither this, nor a similar work, has been published or presented to an examination committee.

Dresden, August 8, 2014 Jakob Schneider

Erklärung

Hiermit erkläre ich, dass ich die am 8. August eingereichte Bachelorarbeit zum Thema *Complete Arcs in Projective Spaces, the MDS Main Conjecture and Related Problems* unter Betreuung von Prof. Dr. Ulrich Brehm selbstständig erarbeitet, verfasst und Zitate kenntlich gemacht habe. Andere als die angegebenen Hilfsmittel wurden von mir nicht benutzt.

Dresden, 8. August, 2014 Jakob Schneider

Acknowledgement

I want to thank Sebastian Manecke for some linguistic corrections. Furthermore, I wish to thank my supervisor Prof. Dr. Ulrich Brehm for useful advice, which hopefully increased the comprehensibility of my work, and Prof. Dr. Gerhard Röhrle as well as Dr. Torsten Hoge who gave me an idea about a connection of the MDS main conjecture and Zaslavsky's lemma. Lastly, I would like express my gratitude to Susanne Stimpert for a useful conversation helping me to clean my mind and to complete this thesis.

Contents

Preliminaries

The topic of this thesis first came to my mind when I set up my three hard drives to work together as a RAID[1]. Although the linear code behind this so-called RAID5 level is of extreme simplicity, the principle itself (i.e. the notion of optimal redundancy) turns out to admit highly interesting mathematical aspects.

The notion behind optimal redundancy in a RAID consisting of n hard drives but storing only the information of k hard drives ($k \leq n$) is as follows. Whenever $l \leq n-k$ hard drives stop to work the computer shall still be able to recover the information from the remaining $n-l$ ones. Actually, this means that any k hard drives carry the full information and thus it is somehow 'ideally distributed' among the hard drives.

Certainly, there are many ways to treat the above problem mathematically — but the simplest among these seems to be the concept of MDS codes. Here, we associate to any of the n hard drives a row in the generator matrix of an (n,k)-MDS code (i.e. the minimum weight of the code is $n-k+1$). The statement that the whole information can be recovered from any k hard drives then translates to the property of the generator matrix that any $k \times k$-submatrix of it is regular.

Of course, one could consider the above over an arbitrary ring, but for the sake of simplicity of calculation it is self-evident to restrict oneself to a field. Moreover, finite fields are most natural to use when processing 'digital' data with computers — especially fields of charactaristic two.

Now, having agreed on the finite field $\mathbb{F}_q$ of q elements, we can ask which ratios k/n we can attain. Regrettably, as it often seems to be the case — small charactaristic does complicate this problem a lot.

The conjecture arising from this last question is the so-called 'MDS main conjecture' which was first stated in 1955 by Beniamino Segre and remains open until today.

However, an astonishing new result contributing to the answer of this problem was recently published by Simeon Ball and Jean De Beule which gives an affirmative answer to this question in the case of prime fields. In particular, the methods used in their paper [1] (and in the subsequent paper [3]) are of completely elementary nature. We will simplify some 'technical aspects' of the proofs given in these two papers and present them appropriately to the reader, (cf. Section 5).

This section can also be seen as the core part of the thesis.

The structure of the thesis is as follows: In Section 1 (p. 1) we start with some elementary combinatorial considerations of some sets in finite projective geometry which are somehow related to the concept of projective arcs and are natural to consider in this context (these are (k,m)-arcs and hyperovals). In Section 2 we introduce the notion of a *projective arc* and draw connections to some 'equivalent concepts'. At the end of this section we formulate the MDS main conjecture for these different terms. The following section presents some results which hold in a somehow more general context related to the combinatorial aspects of so-called *generic* and *weakly generic* hyperplane arrangements which are closely related to MDS codes as we will have seen in the previous section. The results presented here are some simple generalizations of some facts proven by Zaslavsky in [8].

In Section 4 we present the most common class of $(q+1)$-arcs and their coding theoretic

[1] redundant array of independent disks

version. Especially, we construct the most relevant representations of these (and generator matrices of related codes). Moreover, we investigate whether they are complete in some cases.

The subsequent section forms — as we already mentioned — the core part of the thesis presenting the proof (and classification of $(q+1)$-arcs) of the MDS main conjecture for $n \leq p$ and $n \leq 2p-2$ (without classification) given by Simeon Ball and Jean De Beule which is in my opinion of unobtrusive elegance.

Lastly, we draw some connections to the Kneser graphs of type $\mathrm{KG}(2n-3, n-2)$ which offer the possibility of an alternative proof of the conjecture for the case $(n \leq p)$ by looking carefully at the interpolation system of tangent polynomials. Although this connection is not mentioned anywhere, I found it suitable to mention it at this point. But of course we cannot classify the $(q+1)$-arcs using an argument of that type.

There are many aspects related to the topic which are not discussed here — especially when posing the question of maximal arcs in a rather topological context (i.e. in characteristic zero) and also some results I rediscovered which admit a closer relation to the contents of this thesis. However, it is clear that these would certainly have gone beyond the scope of this work.

This thesis is designed to be readable without great effort for an undergraduate student with basic knowledge in projective geometry, group theory and linear algebra.

Jakob Schneider,
August 8, 2014

Notations and Conventions

We want to introduce several notation conventions used throughout the thesis.

Generalized binomial coefficient. Define the generalized binomial coefficient as

$$\binom{n}{k}_q := \prod_{i=1}^{k} \frac{q^n - q^{n-i}}{q^k - q^{k-i}}.$$

This counts the number of $(k-1)$-dimensional projective subspaces of an $(n-1)$-dimensional projective space. In all sections, P denotes the projective functor.

Definition up to scalar factor. When defining a polynomial only up to scalar factor of the underlying field, we write '$:\doteq$' instead of '$:=$'.

Groups. We assume that the reader is familiar with the projective linear group $\mathrm{PGL}(n, K)$, and the projective semilinear group $\mathrm{P\Gamma L}(n, K)$. Moreover, we write the semidirect product of groups A and B as $A \rtimes B$ (via some map $\phi : B \to \mathrm{Aut}\, A$ which is mostly clear form the context) and the wreath product of A and B as $A \wr B$ (here $B \leq S_m$ for some m is understood as a group of permutations and $A \wr B \cong A^m \rtimes B$).

Substructures. By $\operatorname{Sub} A$ we always mean the substructures of a structure as indicated by a substript if necessary (e.g. $\operatorname{Sub}_{\mathbf{Aff}} V$ for a vector space V means the affine subspaces whereas $\operatorname{Sub} V = \operatorname{Sub}_{\mathbf{Vec}} V$ means the linear subspaces of V). Similarly, for a set S with no further algebraic structure explained on it $\operatorname{Sub} S = \operatorname{Sub}_{\mathbf{Set}} S$ just means the powerset of S[2].

Hulls. The hull generated by some subset S of a complete lattice L will also be written as $\langle S \rangle_L$ instead of $\bigvee L$. This notation is especially used for vector spaces (e.g. $\langle S \rangle_{\operatorname{Sub} V}$ means the subspace generated by S of V).

Meets and joins. For most operations which can be interpreted as meet and join of an underlying lattice, we write '$\wedge$' and '$\vee$'. This applies e.g. to the lattice of subspaces of a vector space and the greatest common divisor and least common multiple of natural numbers or polynomials (although these are unique only up to a unit). To express the minimum and maximum of a set of numbers we use min and max.

Vector spaces. When we deal with the vectorspace K^n (where possibly $K = \mathbb{F}_q$) then $e_0, \ldots, e_{n-1}$ always denotes the standard basis, i.e.

$$e_i := (\delta_{ij})_{j=0}^{n-1} .$$

Moreover, when $x_0, \ldots, x_{n-1}$ is a basis of a (finite dimensional) vector space by $x_0^*, \ldots, x_{n-1}^*$ we mean its dual basis, i.e.

$$x_i^*(x_j) = \delta_{ij}.$$

Permutations and sequences. In Section 5 we will make exhaustive use of sequences (or permutations) of vectors. For this reason we introduce the following convention. For any given set $\mathcal{A}$ on which we have assigned a total order $\leq$ by the term $(A_0, \ldots, A_{n-1})$ we mean the sequence given by writing down the elements of $A_0, \ldots, A_{n-1}$ each in the order given by $\leq$. For convenience we write singletons without curly brackets (e.g. $(\{1,5,4\}, 2, \{6,3\}) = (1,4,5,2,3,6)$ where the numbers are ordered by size).

Signs and determinants. Given a $(a_i)_{i=0}^{m-1}$ where all a_i are distinct and $a_i \in \mathcal{A}$ for some totally ordered set $\mathcal{A}$ we define the sign of this sequence with respect to the order declared on $\mathcal{A}$ as the sign of the permutation $(a_i)_{i=0}^{m-1}$ of $\left(\{a_i\}_{i=0}^{m-1}\right)$. Similarly, we can apply the determinant det to an n-sequence of vectors of an n-dimensional vectorspace — where the former is of course always taken with respect to some fixed basis $(e_i)_{i=0}^{n-1}$.

[2]More generally, we assign multiple meanings to symbols indicating the current interpretation by a subscript of the operator applied to it if necessary

1 Combinatorics of sets in finite projective space

1.1 (k, m)-arcs in projective planes

We start with some objects in the projective plane — however we introduce them a bit more generally.

Definition 1.1 ((k, m)-arc). Let P be a projective space of order q. Then a set $\mathcal{A}$ will be called a (k, m)-*arc* if $|\mathcal{A}| = k$ and any line l of P intersects $\mathcal{A}$ in at most m points.

Definition 1.2 ((m, n)-secant). Let $\mathcal{S} \subseteq P$ be a subset of some projective space P. Then a subspace of (projective) dimension n intersecting $\mathcal{S}$ in exactly m points is called an (m, n)-*secant* of $\mathcal{S}$. In the case we are dropping the n we mean a line. Moreover, a 2-secant will also be denoted as a *bisecant*, a 1-secant as a *tangent* and a 0-secant as an *external line*.

Remark 1. Thus a (k, m)-arc in a plane π is just a k-set having no m'-secants for $m' > m$.

A very natural question (and also the main question in this entire thesis but stated for different objects) is clearly which values k can be attained for a given order q of the plane and parameter m.

A simple bound for k is given by the following general fact

Lemma 1.1 (size of (k, m)-arcs). *Let $\emptyset \neq \mathcal{A} \subseteq P$ be a (k, m)-arc and the space P be of order q and dimension n. Then it holds that*

$$k = |\mathcal{A}| \leq \binom{n}{1}_q (m - 1) + 1$$

where equality occurs if and only if any line in P meets $\mathcal{S}$ in either 0 or m points.

Proof. Pick a point $p \in \mathcal{A}$. There are $\binom{n}{1}_q$ lines through p each of which carries at most $m - 1$ other points of $\mathcal{S}$. This gives the desired bound and conversely if this bound is attained a line passing through an arbitrary point $p \in \mathcal{S}$ must clearly pass through $m - 1$ other points of $\mathcal{A}$. □

However, whether or not this bound is actually attained is no simple question, already in the case where $n = 2$, disregarding the cases where $m = q + 1$ or $m = 1$ (the above estimate requires $\mathcal{A}$ not to be empty).

Definition 1.3. A (k, m)-arc in projective space P is called *maximal* if it attains the bound of the Lemma 1.1. It is called *complete* if it is maximal with respect to inclusion among all (k, m)-arcs in P.

We might apologize for this somehow confusing definition by refering to the literature. Actually, to revisit this last question one may observe that it sufficies to answer it in small dimensions (when q is odd we will see that it sufficies to answer this question for $n = 2$ for which Thas

conjectured in 1975 that there are no maximal (k,m)-arcs in odd planes, which was proven by S. Ball, A. Blukhuis and F. Mazzocca in [2]).

Lemma 1.2. *Let $\mathcal{A}$ be a maximal (k,m)-arc in projective space P and $P' \leq P$ having non-empty intersection with $\mathcal{A}$. Then the points of $\mathcal{A}$ lying in P' form another maximal (k',m)-arc.*

Proof. Using Lemma 1.1, we obtain that for any point $p \in \mathcal{A} \cap P'$ all lines through p contain m points showing that $\mathcal{A} \cap P'$ is maximal by that same fact. □

It is thus clear that the non-existence of maximal (k,m)-arcs in some dimension implies the non-existence in all higher dimensions (for Desarguian spaces).

We now turn to the case of a projective plane.

Lemma 1.3 (dual (k,m)-arc). *Let $\mathcal{A}$ be a maximal (k,m)-arc in the plane π such that $\mathcal{A} \notin \{\emptyset, \pi\}$ and $\mathcal{A}'$ be the set of external lines of $\mathcal{A}$. Then $\mathcal{A}'$ is a maximal $(k', \frac{q}{m})$-arc in the dual plane (in particular $m|q$).*

Proof. Let E_p be a set of external lines of $\mathcal{A}$ intersecting at $p \in \pi \setminus \mathcal{A}$. Let L_p be the lines incident with p. Then we have that $|L_p \setminus E_p|\, m = k$ since $\mathcal{A}$ is maximal (Lemma 1.1). Thus we deduce that

$$|E_p| = \binom{2}{1}_q - \frac{k}{m} = \frac{(q+1)m - ((q+1)(m-1)+1)}{m} = \frac{q}{m}.$$

Lastly, we may compute k' by a double counting argument

$$\begin{aligned} k' &= \frac{1}{q+1} \sum_{p \in P \setminus \mathcal{A}} |E_p| = \frac{q}{m} \frac{q^2+q+1-(qm+m-q)}{q+1} \\ &= \frac{q(q+1)}{m} - q, \end{aligned}$$

as through every point in $P \setminus \mathcal{A}$ pass q/m external lines, and any of these external lines carries $q+1$ points. □

Hence, non-trivial maximal arcs can only exist for $m|q$. Indeed, this is the case for q even, as in this case one can construct the so called Denniston arcs.

Lemma 1.4. *Let $\pi = \mathrm{P}\mathbb{F}_q^3$ be a Desarguian projective plane of order $q = 2^e$. Then there exist maximal (k,m)-arcs for each $m|q$.*

Proof. Consider the affine plane $\mathbb{F}_q^2$ embedded in π. Since $m|q$ there as a subgroup $H \subseteq \mathbb{F}_q$ of order m of the additive group (which is an elementary Abelian p-group). Choose an irreducible homogeneous quadratic polynomial $\gamma(X,Y)$ on $\mathbb{F}_q^2$. Then $\mathcal{A} := \{(x,y) \in \mathbb{F}_q^2 : \gamma(x,y) \in H\}$ defines a maximal (k,m)-arc. Any affine line which is parameterized by $l : x \mapsto (x, \alpha x + \beta)$ (w.l.o.g. we can express y as a function of x) plugged into the equation $\gamma(X,Y) = aX^2 + bXY + cY^2 \in H$ gives an equation of the type $(a + b\alpha + c\alpha^2)x^2 + b\beta + c\beta^2 \in H$ where the coefficient in front

of x cannot vanish since otherwise γ would admit a projective zero $\langle(1,\alpha)\rangle$. But this equation clearly has exactly $|H| = m$ solutions (since the FROBENIUS map $x \mapsto x^2$ is a bijection). Thus any affine line intersects $\mathcal{A}$ in m points and the line at infinity does not intersect $\mathcal{A}$ at all. □

This is the proof from [4, p. 120] with some additional notes.

As a corollary of Lemma 1.3 (p. 2) it follows that there are no $(q+2)$-arcs in planes of odd order — a first (however simple) result which hints to the MDS main conjecture.

However, in even planes things are quiet different. We discuss this next.

1.2 Ovals and hyperovals

Definition 1.4 (oval). Let π be a projective plane π of order q. An oval $\mathcal{O}$ in π is a $(q+1)$-arc in π.

We already mentioned it, but to fix it as a fact, we have the following

Lemma 1.5 (maximality of ovals if q odd). *Let $\mathcal{O}$ be an oval in a projective plane π of odd order q. Then $\mathcal{O}$ is a maximal arc.*

Proof. Apply Lemma 1.3 (p. 2) for $m = 2$ and q odd. □

The more interesting object we want to discuss briefly is introduced by

Definition 1.5 (hyperoval). Let π be an even plane. A $(q+2)$-arc $\mathcal{O}$ is called *hyperoval*.

Remark 2. Clearly, an oval is a maximal $(q+2, 2)$-arc.

Lemma 1.6. *Let π be an even plane, and $\mathcal{O}$ be an oval. Then $\mathcal{O}$ uniquely extends to a hyperoval by a point $n \in \pi$ called the* nucleus *of $\mathcal{O}$.*

Proof. We have to show that all $q+1$ tangents of $\mathcal{O}$ meet in a unique point. Let $p \in \pi \setminus \mathcal{O}$, and let t_p be the number of tangents of $\mathcal{O}$ and s_p the number of secants of $\mathcal{O}$ passing through p. Thus as $|\mathcal{O}| = q+1$ we have by a double counting argument

$$q + 1 \equiv 2s_p + t_p \bmod 2$$

showing that the number of tangents passing through p is odd (so non-zero). Thus the $q+1$ tangents cover q^2+q+1 points which shows that they must intersect in a unique point n. This follows from the more general fact that k lines $\mathcal{L}$ in the projective plane cover at most $kq+1$ points where equality occurs if and only if they are concurrent. It can be demonstrated by the three double counting identities in which p_i denotes the number of points lying in exactly i of these lines

$$\sum_{i=1}^{k} p_i = N,\ \sum_{i=1}^{k} i p_i = k(q+1) \text{ and } \sum_{i=1}^{k} i(i-1)p_i = k(k-1)$$

where we count the number of points of $\bigcup \mathcal{L}$, the pairs (l, p) of lines of $\mathcal{L}$ and points $\bigcup \mathcal{L}$ where l is incident with p and the pairs $(l, l') \in \mathcal{L}^2$ of distinct (intersecting) lines. Subtracting the first from the second identity and multiplying the result by k yields

$$\sum_{i=1}^{k} k(i-1)p_i = k(k(q+1) - N) \geq \sum_{i=1}^{k} i(i-1)p_i = k(k-1)$$

where equality occurs if and only if $p_i = 0$ for $i = 2, \ldots, k-1$ and so $p_k = 1$. In that case $N = kq + 1$. □

For the sake of completeness, we prove another fact about hyperovals in Desarguian planes.

Lemma 1.7. *Let $\mathcal{O}$ be a hyperoval in a Desarguian plane π. Then $\mathcal{O}$ is* PGL*-equivalent to some oval admitting a representation*[3]

$$\mathcal{C} := \{e_1, e_2\} \cup \left\{ \begin{pmatrix} 1 \\ z \\ f(z) \end{pmatrix} : z \in \mathbb{F}_q \right\},$$

*where $f(z)$ is an $\mathcal{O}$-*polynomial*, i.e. $x \mapsto f(x)$ and $h \mapsto \frac{f(x+h)-f(x)}{h}$ permute $\mathbb{F}_q$ and ${\mathbb{F}_q}^\times$, respectively. Moreover, one may assume that $f(0) = 0$ and $f(1) = 1$.*

Proof. It is well-known that the projective general linear group $\mathrm{PGL}(n, \mathbb{F}_q)$ acts transitively on the $(n+1)$-sets in general position of $\mathrm{P}\mathbb{F}_q^n$. Thus we may assume that the four vectors e_0, e_1, e_2 and $e_0 + e_1 + e_2$ are part of our representation (using an appropriate element of $\mathrm{PGL}(3, \mathbb{F}_q)$). Using an appropriate scalar, we can achieve that the first coordinates of all vectors apart from e_1 and e_2 are one (as they are not zero for otherwise the corresponding vector would be coplanar with e_1 and e_2). Since otherwise two of these vectors would be coplanar with e_1 the third coordinates of them must all be distinct. For the same reason, the second coordinates of two of these vectors must also be distinct else they would be coplanar with e_2. Hence, f is defined and a permutation. Lastly, evaluating the determinants of of triples of vectors in which e_1 and e_2 do not occur we obtain

$$\det \begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ f(a) & f(b) & f(c) \end{pmatrix} = (a-c)f(b) + (b-a)f(c) + (c-b)f(a) \neq 0$$

which leads to

$$(f(a) - f(b))(a - c) \neq (f(a) - f(c))(a - b)$$

or equivalently $h \mapsto \frac{f(x+h)-f(x)}{h}$ is injective for all $x \in \mathbb{F}_q$. □

Using this fact the following hyperovals are natural to discover and B. Segre was the first who did.

[3] here by a representation we mean a system of representatives of the one-dimensional subspaces

Corollary 1 (translation hyperovals). Let $q = 2^e$. Then the set

$$\mathcal{C} := \{e_1, e_2\} \cup \left\{ \begin{pmatrix} 1 \\ z \\ f(z) \end{pmatrix} : z \in \mathbb{F}_q \right\},$$

where $f(z) = z^{2^i}$ is a representation of a hyperoval if and only if $i \wedge e = 1$.

Proof. Clearly, as f is a field automorphism, it is a permutation polynomial. Moreover, the map $h \mapsto \frac{f(x+h)-f(x)}{h} = h^{2^i-1}$ is injective if and only if $(2^i - 1) \wedge (2^e - 1) = 2^{i \wedge e} - 1 = 1$ which holds if and only if $i \wedge e = 1$ (here we use that ${\mathbb{F}_q}^\times$ is cyclic). □

Other hyperovals, which can be discovered in a similar manner are given by the subsequent corollary.

Corollary 2. The polynomial $f(z) = z^6$ is an $\mathcal{O}$-polynomial over $\mathbb{F}_q$ where $q = 2^e$ and e is odd.

Proof. The equation $x^3 - y^3$ factors into $(x - y)(x^2 + xy + y^2)$. But the equation $x^2 + xy + y^2$ is irreducible for e odd since otherwise the field extension $\mathbb{F}_q/\mathbb{F}_2$ would have even degree. Thus $x \mapsto x^2$ and $x \mapsto x^3$ are injective and so f as their composition.

Now we show that $f_x : h \mapsto \frac{f(x+h)-f(x)}{h} = (x^2 + xh + h^2)^2 h$ is injective on ${\mathbb{F}_q}^\times$ (in fact it is injective as a polynomial on the whole $\mathbb{F}_q$). The expression

$$\frac{f_x(h) - f_x(h')}{h - h'} = x^4 + x^2(h^2 + hh' + h'^2) + (h^4 + h^3h' + h^2h'^2 + hh'^3 + h'^4)$$

as a polynomial has only the trivial zero $(x, h, h') = (0, 0, 0)$ we can write it as $(x^2 + \alpha x + \beta)^2$ for

$$\alpha = (h^2 + hh' + h'^2)^{q/2}$$

and

$$\beta = (h^4 + h^3h' + h^2h'^2 + hh'^3 + h'^4)^{q/2}$$

(here we use again the fact that the Frobenius map is surjective for finite fields). Substituting $a := h + h'$ and $b := (hh')^{q/2}$ we get $\alpha = a + b$ and $\beta = a^2 + ab + b^2$. Assume now that $p = x^2 + \alpha x + \beta$ factors. Then its zeros must be of the form $a + c$ and $b + c$ (since their sum is $a + b$). Moreover, by Vieta's formulae they must satisfy

$$(a + c)(b + c) = ab + (a + b)c + c^2 = a^2 + ab + b^2$$

implying that $c^2 + (a + b)c + (a + b)^2 = 0$. But this is possible only if $c = a + b = 0$ since $x^2 + xy + y^2$ was irreducible over our field. However $a = b$ implies that $h^2 + hh' + h'^2 = 0$ which holds only for $h = h' = 0$. So $x = 0$. □

The classification of $\mathcal{O}$-polynomials (which is equivalent to the classification of hyperovals) is still far from being complete. Indeed, one knows a few infinite families of $\mathcal{O}$-polynomials and their disjointness for large enough values of q. For more information on this subject consult [5].

2 The MDS main conjecture

In this section we come to a very interesting open problem which is formulated in coding theory, finite projective geometry, the theory of hyperplane arrangements and matroid theory.

2.1 Projective arcs

We now introduce another concept which coincides with the one of a (k, m)-arc (see Definition 1.3 (p. 1)) in dimension two for $m = 2$.

Definition 2.1 (projective arc). A set $\mathcal{A} \subseteq \mathrm{P}K^n$ is called a *projective arc* if no n points of $\mathcal{A}$ lie in a common hyperplane (if we aim to emphasize the number of points in $\mathcal{A}$ we call it a k-arc when $|\mathcal{A}| = k$). A set $\mathcal{A}' \subseteq K^n$ such that $\mathcal{A} \coloneqq \{\langle a\rangle : a \in \mathcal{A}'\}$ is a projective arc and $\langle a\rangle \neq \langle b\rangle$ for $a, b \in \mathcal{A}'$ is called a *representation* of the arc $\mathcal{A}$.

Remark 3. As we consider only Desarguian spaces, the above definition is not given for non-Desarguian planes.

For the classification of projective arcs it makes sense to consider them under some natural equivalence relations, such as the ones induced by PGL or PΓL. We call two arcs PGL-*equivalent* or PΓL-*equivalent* if there are elements of the corresponding groups mapping one to the other (as a set).

Apart from the 'duality principle' for maximal (k, m)-arcs there is another duality principle for projective arcs.

Definition 2.2 (dual projective arc). Let $\mathcal{A} \subseteq K^n$ a representation of a projective arc in $\mathrm{P}K^n$ and $n + 1 \leq |\mathcal{A}|$. Consider the canonical map

$$\pi : \bigoplus_{a\in\mathcal{A}} Ka \to K^n$$

given by

$$\bigoplus_{a\in\mathcal{A}} \lambda_a a \mapsto \sum_{a\in\mathcal{A}} \lambda_a a$$

and define

$$\pi_a : \bigoplus_{a'\in\mathcal{A}} Ka' \to K$$

as the projection to the summand a. Choose a basis $\mathcal{B}$ of $\ker\pi$. Then

$$\mathcal{A}' \coloneqq \left\{ \sum_{b\in\mathcal{B}} (\pi_a b)b : a \in \mathcal{A} \right\}$$

is a representation of a projective arc in $\ker\pi \cong K^{|\mathcal{A}|-n}$. This is called the *dual arc* of the one represented by $\mathcal{A}$.

Remark 4. Of course this definition depends on the choice of the basis $\mathcal{B}$, but it defines the dual arc up to PGL-equivalence.

We are left to prove that $\mathcal{A}'$ is indeed a representation of projective arc in $\ker \pi \cong K^{|\mathcal{A}|-n}$.

Proof. Consider a non-trivial linear combination of elements of $\mathcal{A}'$ which evaluates to zero.

$$\sum_{a\in\mathcal{A}} \lambda_a \sum_{b\in\mathcal{B}} (\pi_a b)b = \sum_{b\in\mathcal{B}} \left(\sum_{a\in\mathcal{A}} \lambda_a(\pi_a b) \right) b = 0.$$

As $\mathcal{B}$ is linearly independent, we have

$$\left(\sum_{a\in\mathcal{A}} \lambda_a \pi_a \right) b = 0$$

for all $b \in \mathcal{B}$ — that is $\ker \pi \subseteq \ker \sum_{a\in\mathcal{A}} \lambda_a \pi_a$. But any element of $c \in \ker \pi$ must either be zero or at least $n+1$ summands $\pi_a c$ of it do not vanish ($a \in \mathcal{A}$). As $|\mathcal{A}| > n$ we have $\ker \pi \neq 0$ and it follows that $\lambda_a \neq 0$ for at least $|\mathcal{A}| - n + 1$ elements $a \in \mathcal{A}$. Assume the contrary, that $\lambda_a \neq 0$ for $a \in A \subseteq \mathcal{A}$ with $|A| \leq |\mathcal{A}| - n$. Then choose an $(n+1)$-subset B of $\mathcal{A}$ such that $B \cap A = \{c\}$ and a non-trivial linear combination $\sum_{b\in B} \mu_b b = 0$ with $\mu_c \neq 0$. This implies that $\bigoplus_{b\in B} \mu_b b \in \ker \pi$ and

$$\left(\sum_{a\in A} \lambda_a \pi_a \right) \left(\bigoplus_{b\in B} \mu_b b \right) = \lambda_c \mu_c \neq 0,$$

a contradiction showing that any $|\mathcal{A}| - n$ elements of $\mathcal{A}'$ are linearly independent. □

The duality principle for projective arcs is completely analogous to the duality principle for MDS codes (see Definition 2.9). When $\mathcal{A}$ is an arc we write $\mathcal{A}^*$ for its dual arc.

A simple fact which is implied by the above is the following

Corollary 3. Let $\mathcal{A}$ be a projective arc in $\mathrm{P}\mathbb{F}_q^n$ where $q \leq n$. Then $|\mathcal{A}| \leq n+1$ and all maximal examples with respect to cardinality are PGL-equivalent to $\{\langle e_0\rangle, \ldots, \langle e_{n-1}\rangle, \langle e_0 + \cdots + e_{n-1}\rangle\}$. Moreover, $\mathcal{A}$ is extends to such an arc.

Proof. Assume that $\mathcal{A}$ is a projective arc in $\mathrm{P}\mathbb{F}_q^n$ of cardinality $n+2$. Then $\mathcal{A}^*$ has the same cardinality in is a projective arc in $\mathrm{P}\mathbb{F}_q^2$ — thus $|\mathcal{A}^*| \leq q+1$ (as there are only $q+1$ one-dimensional linear subspaces of $\mathbb{F}_q^2$). This implies $|\mathcal{A}| = n+2 \leq q+1$ so $n < q$. The second claim follows from the fact that $\mathrm{PGL}(n, K)$ acts sharply transitive on the $(n+1)$-tuples in general linear position. We briefly demonstrate this. Let $(a_i)_{i=0}^n$ and $(b_i)_{i=0}^n$ be in general linear position. We may assume then that $a_0 = \sum_{i=1}^n \lambda_i a_i$ and $b_0 = \sum_{i=1}^n \mu_i b_i$ ($\lambda_i, \nu_i \in K^\times$, $i = 1, \ldots, n$). A preimage $A \in \mathrm{GL}(n, K)$ of an element $B \in \mathrm{PGL}(n, K)$ which sends $\langle a_i\rangle$ to $\langle b_i\rangle$ must map a_i to $\nu_i b_i$ ($\nu_i \in K^\times$, $i = 0, \ldots, n$). By linearity of A it follows from

$$Aa_0 = A\left(\sum_{i=1}^n \lambda_i a_i \right) = \nu_0 b_0 = \nu_0 \left(\sum_{i=1}^n \mu_i b_i \right) = \sum_{i=1}^n \lambda_i \nu_i b_i$$

that $\nu_i = \nu_0 \frac{\mu_i}{\lambda_i}$ for $i = 1, \ldots, n$. Thus A is defined up to scalar factor $\nu_0 \in K^\times$ so B exists uniquely. The third claim is obvious. □

2.2 Generic hyperplane arrangements

We start by introducing a new concept.

Definition 2.3 (generic and central generic hyperplane arrangement). An arrangement $\mathcal{A}$ of (affine) hyperplanes in $V = K^n$ is called *generic* if for any set of hyperplanes $\mathcal{H} \subseteq \mathcal{A}$ it holds that $\operatorname{codim}_{\mathbf{Aff}} \bigcap \mathcal{H} = |\mathcal{H}|$ if $|\mathcal{H}| \leq n$ and $\bigcap \mathcal{H} = \emptyset$ otherwise. Similarly, $\mathcal{A}$ is called a *central generic arrangement* if for any set of hyperplanes $\mathcal{H} \subseteq \mathcal{A}$ we have $\operatorname{codim} \bigcap \mathcal{H} = \min\{n, |\mathcal{H}|\}$.

Remark 5. It is then clear that the concept of a central generic arrangement is the same as the concept of an arc in $\mathrm{P}V^*$ via the map associating a linear form with its kernel.

We will get back to this interpretation a little later in Section 3 and in the formulation of the MDS main conjecture.

2.3 Linear codes and the Singleton bound

Recall the following definitions

Definition 2.4 ((n,k)-linear code). A linear code of length n and rank k (also denoted as (n,k)-linear code) over a field K is a k-dimensional subspace of K^n.

Definition 2.5. Let $\mathcal{C} \leq K^n$ be linear code. A *generator matrix* G of $\mathcal{C}$ is a matrix having as its rows the coordinate vectors of a basis of $\mathcal{C}$ (with respect to the canonical basis of K^n). A *check matrix* H of $\mathcal{C}$ is a fully ranked matrix having as its kernel the coordinate vectors of $\mathcal{C}$.

As for projective arcs it is meaningful to introduce equivalence relations for linear codes, too.

Definition 2.6. Let $\mathcal{C}, \mathcal{C}'$ be a (n,k)-linear codes over K^n. Then we say $\mathcal{C}$ and $\mathcal{C}'$ are $K^\times \wr S_n$-equivalent or $(K^\times \rtimes \operatorname{Aut} K) \wr S_n$-equivalent if there are elements of the corresponding groups acting by multiplication, application of a field automorphism and permutation on the coordinates mapping $\mathcal{C}$ to $\mathcal{C}'$.

Definition 2.7 (minimum weight and Hamming distance). The Hamming *distance* d_H is a metric on K^n given by

$$d_H(a,b) \coloneqq |\{i \in n : a_i \neq b_i\}|$$

for $a, b \in K^n$ where the a_i and b_i denote the coordinates of a and b in the canonical basis. Similarly, we define

$$w_H(a) \coloneqq d_H(a,0)$$

as the Hamming distance to zero and call it the *weight* of a. Moreover, the Hamming *weight* or *minimum weight* $d(\mathcal{C})$ of an (n,k)-linear code is the minimum Hamming distance between two

of its points. This is

$$d(\mathcal{C}) \coloneqq \min\{w_H(c) : c \in \mathcal{C} \setminus \{0\}\},$$

since d_H is obviously additively invariant. An (n,k)-linear code with HAMMING weight d is also denoted as an (n,k,d)-linear code.

We are interested in special linear codes called MDS codes. To see from where they arise, consider the following lemma.

Lemma 2.1 (SINGLETON bound). *Let $\mathcal{S} \subseteq \mathbb{F}_q^n$ be a set such that any two distinct points of $\mathcal{S}$ have at least HAMMING distance d. Then*

$$|\mathcal{S}| \leq q^{n-d+1}.$$

Similarly, an (n,k)-linear code $\mathcal{C}$ over an arbitrary field K with $d(\mathcal{C}) \geq d$ has dimension $k \leq n-d+1$.

Proof. Consider the projection map $\pi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-d+1}$ which forgets $d-1$ coordinates. Then π is injective on $\mathcal{S}$ since otherwise $\mathcal{S}$ would have two distinct points differing in less than d coordinates contradicting the assumptions, proving the first claim. The second claim follows analogously from the fact that $\pi : K^n \to K^{n-d+1}$ maps $\mathcal{C}$ injectively into a $(n-d+1)$-dimensional space showing that $\dim \mathcal{C} \leq n-d+1$. This finishes the proof. □

This motivates the definition of MDS codes.

Definition 2.8 (linear MDS code). An (n,k,d)-linear code $\mathcal{C}$ is called *maximum distance separable* or (n,k)-*MDS code* if the singleton bound is fulfilled with equality, i.e. $k = n-d+1$.

A very important concept for linear codes and especially for MDS codes is *duality*.

Definition 2.9 (dual code). Let $\mathcal{C} \leq K^n$ be a linear code of dimension k. The *dual code* $\mathcal{C}^*$ of $\mathcal{C}$ is defined as $\mathcal{C}^* \coloneqq \{c^* \in K^{n*} : \mathcal{C} \leq \ker c^*\}$. The dual code is thus of codimension k.

Remark 6. It is thus clear that a generator matrix G of $\mathcal{C}$ is a check matrix of $\mathcal{C}^*$ and vice versa.

We can characterize the minimum weight of a code via its check and generator matrices.

Lemma 2.2 (Characterization of the minimum weight via associated matrices). *Let $\mathcal{C} \leq K^n$ be a linear code of dimension k. Then $\mathcal{C}$ has minimum weight d if and only if one of the following conditions holds true.*

(I) For any check matrix $H \in K^{(n-k)\times n}$ of $\mathcal{C}$ the number d is the minimal number of linear dependent columns of H. Or alternatively, $d-1$ is the maximum of the numbers $e \in \mathbb{N}$ such that any e columns of H are linearly independent.

(II) For any generator matrix $G \in K^{k\times n}$ of $\mathcal{C}$ the number $n-d$ is the maximal number of columns of G such that the rows of the submatrix corresponding to these columns are linearly dependent. Or alternatively, $n-d+1$ is the minimum of the numbers $f \in \mathbb{N}$ such that any submatrix of G consisting of f columns has linearly independent rows.

Proof.

(I): Each vector $(c_0, \ldots, c_{n-1})$ corresponds to a linear combination $\sum_{i=0}^{n-1} c_i h_i$ where h_i are the columns of H. Thus each non-zero vector $c \in \mathcal{C}$ corresponds to a non-trivial linear combination of columns of H.

(II): Similarly, if G is a generator matrix then any non-zero vector $c \in \mathcal{C}$ can be uniquely written as $c = G^\top x$ for $x \in K^k$. Thus any vector $c \in \mathcal{C} \setminus \{0\}$ having weight w corresponds to a $k \times (n-w)$-submatrix of G having linearly dependent rows.

Hence, we are done with the proof. □

It is now easy to characterize linear MDS codes via their associated matrices.

Lemma 2.3 (characterization of MDS codes). *Let $\mathcal{C}$ be an (n,k,d)-linear code. Then the following are equivalent*

(I) $\mathcal{C}$ is MDS.

(II) A check matrix $H \in K^{(n-k)\times n}$ has the property that any maximal square submatrix of it is regular.

(III) A generator matrix $G \in K^{k\times n}$ has the property that any maximal square submatrix is regular.

(IV) The dual code $\mathcal{C}^*$ is MDS.

Proof.

(I) $\Leftrightarrow$ (II): The property of $\mathcal{C}$ that $d(\mathcal{C}) = d = n-k+1$ implies the property of a check matrix H of $\mathcal{C}$ that any $(n-k)\times(n-k)$-submatrix of H has independent rows and is thus regular by the previous lemma. On the other hand, if every such matrix is regular then its rows are linearly independent and so $d-1 \geq n-k$ again by Lemma 2.2. But $d-1 \leq n-k$ holds as well by the SINGLETON bound.

(I) $\Leftrightarrow$ (III): The property of $\mathcal{C}$ that $d(\mathcal{C}) = n-k+1$ implies the property of a generator matrix G of $\mathcal{C}$ that any $k\times k$-submatrix of G has linearly independent rows and is thus regular. Conversely, if any $k\times k$-submatrix is regular then its rows are linearly independent and thus by Lemma 2.2 $n-d+1 \leq k$. The reverse inequality again holds by the SINGLETON bound.

(I) $\Leftrightarrow$ (IV): A generator matrix of $\mathcal{C}$ is a check matrix of $\mathcal{C}^*$ and vice versa. By the last two equivalences $\mathcal{C}$ and $\mathcal{C}^*$ can only be MDS codes at the same time.

This completes the proof. □

To fix this interesting type of matrices which are a check (or generator) matrix of an MDS code we make the following

Definition 2.10 (principally regular matrix). A matrix A over some ring R such that any maximal square submatrix of A is regular is called *principally regular matrix*.

There is a very simple connection between this type of matrix and another type of matrix.

Definition 2.11 (totally regular matrix). Let B be a matrix such that any square submatrix of B is regular. Then B is called *totally regular*[4].

We briefly demonstrate the connection between these two types of matrices.

Lemma 2.4 (connection between principally and totally regular matrices). *Let $C \coloneqq (A|B) \in R^{m\times n}$ be some matrix over a ring R and $m \leq n$ where $A \in R^{m\times m}$. Then the following two are equivalent.*

(I) C is principally regular.

(II) A is invertible and $A^{-1}B$ is totally regular.

Proof. We only proof the direction (I) $\Rightarrow$ (II) since the other is obvious. When C is principally regular then A is invertible so that $A^{-1}C$ is also principally regular. Now let $k \leq \min\{m, n-m\}$. Choosing k-sets $I \subseteq \{0,\dots,m-1\} = m$ and $J \subseteq \{m,\dots,n-m-1\} = n \setminus m$ we can check the matrix $A^{-1}C\big|_{m\times(m\setminus I\cup J)}$ for regularity which is easily seen to be equivalent to the fact that $A^{-1}B\big|_{I\times J}$ is regular.

This is mainly based on the fact that the matrix

$$\begin{pmatrix} 1 & X \\ 0 & Y \end{pmatrix}$$

over a ring R is regular if and only if Y is regular and admits the inverse

$$\begin{pmatrix} 1 & -XY^{-1} \\ 0 & Y^{-1} \end{pmatrix}$$

and using an appropriate permutation we can achieve that $A^{-1}C\big|_{m\times(m\setminus I\cup J)}$ is of the upper form and $A^{-1}B\big|_{I\times J}$ corresponds to Y. □

[4]Regrettably, the denotation of these matrices in the literature and different papers is not very consistent

2.4 Connections

Having introduced several probably new concepts and ideas, we now start by drawing some connections between these.

We already saw how MDS codes and principally or totally regular matrices are related. To draw the connection to projective arcs we interpret the one-dimensional subspaces of the columns of a check matrix H of an (n,k)-MDS code over K as elements of the projective space $\mathrm{P}\operatorname{col} H \cong \mathrm{P}K^{d-1}$ (as $d = n-k+1$). This gives us a projective arc of size n which is uniquely determined by the code up to PGL-equivalence (by the choice of the check matrix and by forgetting scalar factors).

Conversely, starting from a projective arc $\mathcal{A}$ in $\mathrm{P}K^{d-1}$ we can reconstruct the original MDS code only up to $K^\times \wr S_n$-equivalence, since the elements of $\mathcal{A}$ are not ordered and a representative of a one-dimensional subspace is only defined up to scalar factor. This shows that $K^\times \wr S_n$-orbits of MDS codes are in a one-to-one relation with PGL-orbits if projective arcs (the same holds for $(K^\times \rtimes \operatorname{Aut} K) \wr S_n$-orbits of MDS codes and PΓL-orbits of projective arcs).

On the other hand, given an arc $\mathcal{A}$ in $\mathrm{P}K^n$ we can get a central generic arrangement $\mathcal{B}$ of hyperplanes by interpreting the elements of $\mathcal{A}$ as (non-zero) linear forms $\mathcal{F}$ in K^{n*} (which can be chosen up to scalar factor). Then $\mathcal{B} \coloneqq \{\ker f : f \in \mathcal{F}\}$ is the associated central generic arrangement. Finally, we can get an (affine) generic arrangement from a non-empty central generic one by a deconing construction. If $P_\mathcal{A}(X_0,\dots,X_{n-1}) = \prod \mathcal{F} \in \mathbb{F}_q[X_0,\dots,X_{n-1}]$ is the defining polynomial of $\mathcal{A}$ with respect to the basis $x_0,\dots,x_{n-1}$ (i.e. $P_\mathcal{A}(x_0^*,\dots,x_{n-1}^*) = \prod_{H\in\mathcal{A}} l_H$ where $\ker l_H = H$) and $\ker x_0^* \in \mathcal{A}$ then the affine generic arrangement $\mathcal{A}^{\mathrm{aff}}$ arising from that by deconing $\mathcal{A}$ has defining polynomial $P_{\mathcal{A}^{\mathrm{aff}}}(X_1,\dots,X_{n-1}) = P_\mathcal{A}(1,X_1,\dots,X_{n-1})$ with respect to the basis $x_1,\dots,x_{n-1}$ of $\pi_{(1,\dots,n-1)}\mathbb{F}_q^n$ (that is the intersection of the hyperplanes in $\mathcal{A}$ with the one given by $x_0 = 1$).

Conjecture 2.1 (main conjecture on MDS codes, projective arcs, generic arrangements in $\mathbb{F}_q^n$). Let $m(n,q)$ be the minimum of all integers m such that $|\mathcal{A}| \le m$ for any arc $\mathcal{A}$ in a projective space of dimension n and order q then

$$m(n,q) = \begin{cases} n+2: & n \ge q \\ q+2: & n \in \{2, q-1\} \wedge 4|q \\ q+1: & \text{otherwise} \end{cases}.$$

Remark 7. We fully proved the conjecture for $n \ge q$ (see Corollary 3 (p. 7)) characterizing the sets $\mathcal{A}$ of maximal cardinality. For $n = 2$ it is (as we have shown) a consequence of Lemma 1.1 (p. 1) and Lemma 1.3 (p. 2) and the classification of sets $\mathcal{A}$ of maximal cardinality in the case of even q or non-Desarguian planes seems to be very difficult. In the case where q is odd and the plane is Desarguian, we will see that these sets $\mathcal{A}$ are precisely non-singular conics (this will be a consequence of Corollary 7).

Remark 8. Equivalently, $m(n,q)-1$ is the minimum of integers m' such that for all generic hyperplane arrangements $\mathcal{B}$ in $\mathbb{F}_q^n$ it holds that $|\mathcal{B}| \le m'$ or $m(k-1,q)$ is minimal among all

m'' such that all (n,k)-MDS codes $\mathcal{C}$ over $\mathbb{F}_q$ satisfy $n \leq m''$. This can easily be seen from the connections we have drawn.

3 Generic hyperplane arrangements

In the following we examine some combinatorial properties of generic and weakly generic hyperplane arrangements. These lead to the somehow obvious bound for a projective arc in $\mathrm{P}\mathbb{F}_q^n$ that $|\mathcal{A}| \leq q+n-1$ by a simple counting argument, however the results we present can be seen as a (simple) generalization of results by Zaslavsky about the number of components of the complement $\mathcal{M}(\mathcal{A}) =: \mathcal{M}_0(\mathcal{A})$ of a real arrangement of hyperplanes $\mathcal{A}$ and its analogue in the discrete case. Moreover, I found it suitable to point out the connection between the topic of hyperplane arrangements and projective arcs.

3.1 Existence of weakly generic arrangements in $\mathbb{F}_q^n$ with given Poincaré polynomial

Let $\mathcal{A}$ be an arrangement of hyperplanes in $V = K^n$ and $\mathcal{L}(\mathcal{A}) := \{\bigcap \mathcal{H} : \mathcal{H} \subseteq \mathcal{A}\}$ the associated lattice, where for $X, Y \in \mathcal{L}(\mathcal{A})$ we define $X \wedge Y := \bigcap\{Z \in \mathcal{L}(\mathcal{A}) : X, Y \subseteq Z\}$ and $X \vee Y := X \cap Y$. Moreover, we assign to $\mathcal{L}(\mathcal{A})$ the rank function $\mathrm{rk} : \mathcal{L}(\mathcal{A}) \to \mathbb{Z}$ where $X \mapsto \operatorname{codim} X$ for $X \neq \emptyset$ and $\mathrm{rk}(\emptyset) := n+1$. It is then an interesting question, which restrictions on the lattice $\mathcal{L}(\mathcal{A})$ arise from the structure of the space K^n (especially when K is finite). We want to discuss this question for a special type of arrangements.

We need the following definitions.

Definition 3.1 (unique representation of lattice elements). Let L be a lattice with 0 (minimal element). Then $X \in L$ is called *uniquely representable* if it can uniquely be written as the join of atoms.

Remark 9. If $X \in \mathcal{L}(\mathcal{A})$ is uniquely representable and $Y \leq X$ then is also uniquely representable.

Definition 3.2 (weakly generic arrangement). Let $\mathcal{A}$ be an arrangement such that any element $X \in \mathcal{L}(\mathcal{A}) \setminus \{\emptyset\}$ is uniquely representable. Then $\mathcal{A}$ is called *weakly generic*.

Definition 3.3. Let $\mathcal{A}$ be an arrangement and $X \in \mathcal{L}(\mathcal{A})$, then denote by $\mathcal{A}^X$ the restricted arrangement on X, i.e. $\mathcal{A}^X := \{X \cap H : \operatorname{codim}_X(X \cap H) = 1\}$.

A fact, which is also obvious is that a lattice $\mathcal{L}$ is the lattice $\mathcal{L}(\mathcal{A})$ for an arrangement $\mathcal{A}$ in K^n if and only it is embedded in $\mathrm{Sub}_{\mathbf{Aff}} V$ (by a rank preserving map). However, it turns out to be very difficult to decide this for a given lattice. We now drop some information and briefly discuss the above question for a weakly generic arrangement $\mathcal{A}$ in K^n with given Poincaré polynomial.

Therefore, it becomes necessary to introduce the following concepts.

Definition 3.4 (Möbius function). Let P be a poset and $I : P \times P \to \mathbb{Z}$ be its *incidence function*, i.e.

$$I(X,Y) \coloneqq \begin{cases} 1 & : X \leq Y \\ 0 & : \text{otherwise} \end{cases}$$

then the Möbius *function* is the inverse matrix of I, i.e.

$$\sum_{Z \in P} \mu(X,Z) I(Z,Y) = \sum_{Z \leq Y} \mu(X,Z) = \delta_{XY}.$$

Remark 10. The fact that the Möbius function always exists is due to the fact that any ordering can be embedded in a total ordering so that $(I(X,Y))_{X,Y}$ can be written as a upper unitriangular matrix. Thus $\mu(X,X) = 1$ and $\mu(X,Y) = 0$ if $X \not\leq Y$.

Definition 3.5 (Poincaré polynomial). Let $\mathcal{A}$ be a hyperplane arrangement. The Poincaré *polynomial* of $\mathcal{A}$ is defined by

$$\pi(\mathcal{A}, t) \coloneqq \sum_{X \in \mathcal{L}(A) \setminus \{\emptyset\}} \mu_{\mathcal{A}}(X)(-t)^{\operatorname{rk} X}$$

where $\mu_{\mathcal{A}}(X) \coloneqq \mu_{\mathcal{A}}(V, X)$ is the Möbius function of the poset $\mathcal{L}(\mathcal{A})$.

3.2 Some combinatorial facts about weakly generic arrangements

Lemma 3.1 (point numbers of the strata $\mathcal{M}_m$ of arrangements in finite vector spaces). *Let $\mathcal{A}$ be a weakly generic arrangement in $\mathbb{F}_q^n$. Then we have*

$$|\mathcal{M}_m(\mathcal{A})| = q^{n-m} \frac{\pi^{(m)}(\mathcal{A}, -q^{-1})}{m!}$$

where $\mathcal{M}_m(\mathcal{A})$ denotes the m-th stratum ($m \geq 0$)

$$\mathcal{M}_m(\mathcal{A}) := \bigcup \{X \in \mathcal{L}(\mathcal{A}) \wedge \operatorname{rk}(X) = m\} \setminus \bigcup \{X \in \mathcal{L}(\mathcal{A}) : \operatorname{rk}(X) = m+1\}.$$

For $m = 0$ the arrangement does not have to be weakly generic (Zaslavsky's result in [8]).

The proof of this fact is just based on Möbius inversion.

Proof. We start with $m = 0$. As $\bigcup_{X \in \mathcal{L}(\mathcal{A})} \mathcal{M}_0(\mathcal{A}^X) = \mathbb{F}_q^n$ (where $\mathcal{A}^X$ denotes the restriction of $\mathcal{A}$ on X) and the union is disjoint we have that (for $Y \in \mathcal{L}(\mathcal{A})$)

$$\sum_{\substack{X \in \mathcal{L}(\mathcal{A}) \\ Y \leq X}} \left|\mathcal{M}_0(\mathcal{A}^X)\right| = \sum_{X \in \mathcal{L}(\mathcal{A})} I(Y,X) \left|\mathcal{M}_0(\mathcal{A}^X)\right| = q^{n - \operatorname{rk}(Y)}.$$

MÖBIUS inversion reveals

$$\sum_{X\in\mathcal{L}(\mathcal{A})} \mu(V,Y)q^{n-\mathrm{rk}(Y)} = q^n\pi(\mathcal{A},-q^{-1}) = |\mathcal{M}_0(\mathcal{A})|\,.$$

This is essentially a result analogue to the lemma proved by ZASLAVSKY in [8]. Note that we did not use that $\mathcal{A}$ is weakly generic. For the case $m>0$ we obtain

$$|\mathcal{M}_m(\mathcal{A})| = \sum_{\substack{X\in\mathcal{L}(\mathcal{A})\\ \mathrm{rk}(X)=m}} \left|\mathcal{M}_0(\mathcal{A}^X)\right| = \sum_{\substack{X\in\mathcal{L}(\mathcal{A})\\ \mathrm{rk}(X)=m}} \sum_{Y\in\mathcal{L}(\mathcal{A}^X)} \mu_{\mathcal{A}^X}(X,Y)q^{n-\mathrm{rk}(Y)},$$

where $\mu_{\mathcal{A}^X}$ is the MÖBIUS function of the restricted arrangement. Now, we use the fact (which can be easily shown by induction) that for a weakly generic arrangement $\mathcal{A}$ we have $\mu(X,Y) = (-1)^{\mathrm{rk}(X)-\mathrm{rk}(Y)}$ and as restrictions of weakly generic arrangements are again weakly generic, we obtain from the above (interchanging the sums and counting the elements X lying below Y).

$$\begin{aligned}|\mathcal{M}_m(\mathcal{A})| &= q^{n-m}\sum_{Y\in\mathcal{L}(\mathcal{A})} (-1)^{m-\mathrm{rk}(Y)}\binom{\mathrm{rk}(Y)}{m} q^{m-\mathrm{rk}(Y)}\\ &= q^{n-m}\frac{\pi^{(m)}(\mathcal{A},-q^{-1})}{m!}\end{aligned}$$

Here, we use that $\mathrm{rk}(Y)$ and $\mathrm{rk}(X)=m$ is equal to the number of atoms (i.e. hyperplanes) whose join is Y or X, respectively. This ends the proof. □

For the sake of completeness, we shall give the real analogue of that last fact.

Lemma 3.2 (number of connected components of the stratum $\mathcal{M}_m(\mathcal{A})$ of an arrangement). *Let $\mathcal{A}$ be a weakly generic arrangement in $\mathbb{R}^n$. Then it holds that*

$$\frac{\pi^{(m)}(\mathcal{A},1)}{m!} = |\mathrm{comp}(\mathcal{M}_m(\mathcal{A}))|\,,$$

where $\mathrm{comp}(\mathcal{M}_m(\mathcal{A}))$ *denotes the components of the m-th stratum. For $m=0$ the arrangement does not have to be weakly generic (see [8]).*

Here, the proof is analogous.

Proof. Starting with $m=0$, EULER's formula gives (for $Y\in\mathcal{L}(\mathcal{A})$)

$$\begin{aligned}\sum_{\substack{X\in\mathcal{L}(\mathcal{A})\\ X\geq Y}} (-1)^{\mathrm{rk}(Y)-\mathrm{rk}(X)}\left|\mathrm{comp}(\mathcal{M}_0(\mathcal{A}^X))\right| &= \sum_{X\in\mathcal{L}(\mathcal{A})} I(Y,X)(-1)^{\mathrm{rk}(Y)-\mathrm{rk}(X)}\left|\mathrm{comp}(\mathcal{M}_0(\mathcal{A}^X))\right| = 1\\ &= \chi(\mathbb{R}^{n-\mathrm{rk}(Y)}).\end{aligned}$$

MÖBIUS inversion delivers

$$\sum_{Y\in\mathcal{L}(\mathcal{A})} \mu(V,Y)(-1)^{\mathrm{rk}(Y)} = \pi(\mathcal{A},1) = |\mathrm{comp}(\mathcal{M}_0(\mathcal{A}))|\,.$$

For $m > 0$, the proof is identical with the last one

$$\begin{aligned}|\mathrm{comp}(\mathcal{M}_m(\mathcal{A}))| &= \sum_{\substack{X\in\mathcal{L}(\mathcal{A})\\ \mathrm{rk}(X)=m}} \left|\mathrm{comp}(\mathcal{M}_0(\mathcal{A}^X))\right| \\ &= \sum_{\substack{X\in\mathcal{L}(\mathcal{A})\\ \mathrm{rk}(X)=m}} \sum_{Y\in\mathcal{L}(\mathcal{A}^X)} \mu_{\mathcal{A}^X}(X,Y)(-1)^{m-\mathrm{rk}(Y)}.\end{aligned}$$

Using that $\mu(X,Y) = (-1)^{\mathrm{rk}(X)-\mathrm{rk}(Y)}$ if $\mathcal{A}$ is weakly generic and as restrictions of weakly generic arrangements are again weakly generic, we obtain from the above

$$\begin{aligned}|\mathrm{comp}(\mathcal{M}_m(\mathcal{A}))| &= \sum_{Y\in\mathcal{L}(\mathcal{A})} \binom{\mathrm{rk}(Y)}{m} \\ &= \frac{\pi^{(m)}(\mathcal{A},1)}{m!}\end{aligned}$$

finishing the proof. □

Remark 11. An alternative proof of these last two lemmas can be given via deletion restriction theorem and the identity $\pi(\mathcal{A},t) = \pi(\mathcal{A}',t) + t\pi(\mathcal{A}'',t)$. The m-th derivative of this last identity behaves analogue to some recurrence relations of the above numbers for $(\mathcal{A},\mathcal{A}',\mathcal{A}'')$ a generic triple of arrangements. For more information on this consult [6].

Corollary 4. Let $\mathcal{A}$ be a weakly generic arrangement in $\mathbb{F}_q^n$. Then it holds that $\pi(\mathcal{A},t) = \pi_q(\mathcal{A},t+q^{-1})$ for a polynomial $\pi_q(\mathcal{A},t)$ with positive coefficients.

This corollary gives a partial answer to our question, but its statement only uses the lattice structure and is careless about the nature of the sets of that lattice (as linear subspaces). It turns out that this answer is not very sharp in some cases.

In particular, when we apply this to a generic arrangement $\mathcal{A}$ in $\mathbb{F}_q^n$ which has Poincaré polynomial

$$\pi(\mathcal{A},t) = \sum_{i=0}^{n} \binom{|\mathcal{A}|}{i} t^i$$

we get for $m = n-1$ that

$$\frac{\pi^{(n-1)}(\mathcal{A},-q^{-1})}{(n-1)!} = \binom{|\mathcal{A}|}{n}\binom{n}{n-1}(-q)^{-1} + \binom{|\mathcal{A}|}{n-1} \geq 0$$

which leads to $|\mathcal{A}| \leq q+n-1$.

This corresponds to a very obvious bound for projective arcs as we will see in Section 5. Better bounds cannot be derived with this simple idea (as the reader might verify by checking the other inequalities which can be derived from the previous lemmas).

4 Extended Reed-Solomon-Codes and normal rational curves

In this section we discuss the most popular (probably) maximal examples of the MDS main conjecture in the case where $\mathcal{A} \subseteq \mathrm{P}K^n$ is an arc for $n \geq 3$ and K a field with $n \leq |K|$.

4.1 Normal rational curves

Definition 4.1 (normal rational curve). A *normal rational curve* is the image of the projective map $\mathrm{P}f : \mathrm{P}K^2 \to \mathrm{P}K^n$ where f is given by

$$(X_0, X_1) \mapsto (X_0^{n-1}, X_0^{n-2}X_1, \ldots, X_0X_1^{n-2}, X_1^{n-1})$$

modulo PGL.

Convention 4.1. For the rest of this section the symbol f denotes the above mapping.

A natural question is whether a normal rational curve is a complete arc. An obvious fact is that it is indeed a projective arc.

Definition 4.2 (projective zeros). Let $p \in K[X_0, X_1]$ be a homogeneous polynomial. We say that $z \in \mathrm{P}K^2$ is a projective zero of p if $z = \langle (z_0, z_1) \rangle$ such that $p(z_0, z_1) = 0$.

Lemma 4.1. *A normal rational curve is a projective arc.*

Proof. Let $l = \sum_{i=0}^{n-1} \lambda_i e_i^*$ be an arbitrary linear form. Then the equation

$$lf(X_0, X_1) = \sum_{i=0}^{n-1} \lambda_i X_0^i X_1^{n-1-i}$$

is a homogeneous polynomial of degree $n-1$ in two variables and thus has at most $n-1$ projective zeros. Thus $\ker l \cap \operatorname{im} \mathrm{P}f$ consists of at most $n-1$ points. □

Notation 4.1 (polynomial coefficients). For a polynomial $p \in R[X_0, \ldots, X_{m-1}]$ we write $[X_0^{e_0} \cdots X_{m-1}^{e_{m-1}}]p$ for the coefficient which is in front of the monomial $X_0^{e_0} \cdots X_{m-1}^{e_{m-1}}$ in p.

Lemma 4.2 (description of $(n-2)$-secant hyperplanes of a normal rational curve). *The hyperplanes $\mathcal{H}$ intersecting a normal rational curve $\mathcal{A} = \operatorname{im} \mathrm{P}f \subseteq \mathrm{P}K^n$ in the representation of Definition 4.1 in exactly the points of an $(n-2)$-set $\mathrm{P}f(A)$ (A is the corresponding $(n-2)$-set of preimages in $\mathrm{P}K^2$) are given as the kernels of the linear forms*

$$l_{A,\alpha} \doteq \sum_{i=0}^{n-1} [X_0^i X_1^{n-1-i}] \left(\det(X, \alpha) \prod_{a \in A} \det(X, a) \right) e_i^*$$

where $\alpha \in A$ and $(e_i)_{i=0}^{n-1}$ denotes the standard basis of K^n and $(e_i^*)_{i=0}^{n-1}$ its dual basis and $X = (X_0, X_1)$, $a = (a_0, a_1)$ ($a \in A$).

Proof. It is clear that the $l_{A,\alpha}(f(a_0,a_1)) = 0$ if and only if $\langle(a_0,a_1)\rangle \in A$. On the other hand, any linear form l, which has as a kernel a hyperplane H with $H \cap \mathcal{A} = A$, must be of the form

$$l = \sum_{j=0}^{n-1} [X_0^i X_1^{n-1-i}] \left(\prod_{a \in A} \det(X,a) \det(X,\alpha') \right) e_i^*$$

since its coefficients in e_i^* can be interpreted as the corresponding coefficients of a homogeneous polynomial in two variables of degree $n-1$. But this polynomial must have all $(n-2)$ elements of A as its zeros (as the assumption on the form l delivers). Hence, there is another zero $\alpha' = \langle(\alpha_0',\alpha_1')\rangle \in \mathrm{P}K^2$ since the polynomial factors into linear polynomials. Since then $\langle f(\alpha_0',\alpha_1')\rangle \in H \cap \mathcal{A} = \mathrm{P}f(A)$ we must have $\alpha' \in A$ (clearly $\mathrm{P}f$ is injective). □

In the sense of the proof of this lemma, we make the following definition. Henceforth, we assume that $\mathcal{A}$ is an incomplete normal rational curve.

Definition 4.3 (associated polynomials and linear forms for incomplete normal rational curves). Assume the normal rational curve $\mathcal{A} \subseteq \mathrm{P}K^n = \mathrm{P}V$ can be extended to a $(q+2)$-arc $\hat{\mathcal{A}} := \mathcal{A} \cup \{\hat{a}\}$ by a point $\hat{a}$. Then for each $(n-2)$-set $A \subseteq \mathrm{P}K^2$ there exists a hyperplane $H_A := \langle \mathrm{P}f(A), \hat{a}\rangle$ and $H_A \cap \hat{\mathcal{A}} = \mathrm{P}f(A) \cup \{\hat{a}\}$. Choose $l_A \in V^*$ such that $\ker l_A = H_A$ and call it an *associated linear form of* A. Define $p_A := \sum_{i=0}^{n-1} l_A(e_i) X_0^{n-1-i} X_1^i$ and call it an *associated polynomial of* A.

Remark 12. Clearly, both p_A and l_A are only determined up to scalar factor from $K^\times$.

Remark 13. The polynomials p_A are precisely the polynomials which are used to construct the forms $l_{A,\alpha}$ in the proof of Lemma 4.2. Thus p_A factors completely into $n-1$ linear factors and has the elements of A as a projective zeros (with one zero of order two).

Definition 4.4. Define P_m as the subspace of $K[X_0,X_1]$ of homogeneous polynomials of degree m.

Lemma 4.3. *The space* $P := \langle p_A \in P_{n-1} : A \subseteq \mathrm{P}K^2, |A| = n-2\rangle_{\mathrm{Sub}\, P_{n-1}}$ *is of dimension* $n-1$.

Proof. The map $\phi : V^* \to P_{n-1}$ mapping associated linear forms to associated polynomials given by $l \mapsto \sum_{i=0}^{n-1} l(e_i) X_0^{n-1-i} X_1^i$ is clearly linear and an isomorphism (the inverse is $p \mapsto \sum_{i=0}^{n-1} ([X_0^i X_1^{n-1-i}]p) e_i^*$ as used in the proof of Lemma 4.2). Thus,

$$\dim P = \dim \langle l_A \in V^* : A \subseteq \mathrm{P}K^2, |A| = n-2\rangle_{\mathrm{Sub}\, V^*}.$$

But the intersection of the kernels of the l_A's contains the extending point $\hat{a} \neq 0$. Hence,

$$\dim \langle l_A \in V^* : A \subseteq \mathrm{P}K^2, |A| = n-2\rangle_{\mathrm{Sub}\, V^*} = n - \dim \bigwedge_{\substack{A \subseteq \mathrm{P}K^2 \\ |A|=n-2}} \ker l_A \leq n-1.$$

On the other hand, we can choose an $(n-1)$-set $B \subseteq \mathrm{P}K^2$ and directly verify that the system of polynomials p_A, where $A \subseteq B$, $|A| = n-2$, is linearly independent by the interpolation formula

$$\left(\sum_{\substack{A \subseteq B \\ |A|=n-2}} \lambda_A p_A \right)(a) = \lambda_{B\setminus\{a\}} p_{B\setminus\{a\}}(a).$$

This proves the linear combination to be trivial if it evaluates to zero (since $p_{B\setminus\{a\}}(a) \neq 0$). Thus,

$$\dim P = \dim \left\langle l_A \in V^* : A \subseteq \mathrm{P}K^2, \left|A'\right| = n-2 \right\rangle_{\mathrm{Sub}\, V^*} = n-1.$$

□

Lemma 4.4. *The space P does not contain a non-zero separable polynomial which splits in $\mathrm{P}K^2$.*

Proof. Assume there is such polynomial p with a set of $n-1$ zeros B. As we have seen in the proof of the previous lemma, the set $\{p_A : A \subseteq B, |A| = n-2\}$ forms a basis of P. Thus we can interpolate p by

$$p = \sum_{a \in A} p(a) \frac{p_{A\setminus\{a\}}}{p_{A\setminus\{a\}}(a)} = 0.$$

A contradiction. □

We thus arrive at a much more 'algebraic' version of the assumption.

Lemma 4.5. *Let $n \leq |K| - 1$. The following two are equivalent.*

(I) A normal rational curve in $\mathrm{P}K^n$ is incomplete.

(II) There is an $(n-1)$-dimensional subspace P of the space P_{n-1} of homogeneous polynomials of degree $n-1$ containing no splitting separable polynomials.

Proof. We have just shown that (I) implies (II). Conversely, if there is a subspace P as described in (II), then it intersects in a one-dimensional subspace with each subspace $P_A := P_1 \prod_{a \in A} \det(X, a)$ (for $A \subseteq \mathrm{P}K^2$ an $(n-2)$-set) — the intersection must be one-dimensional as $\dim P + \dim P_A = n+1$ and $P \vee P_A = P_{n-1}$ since P_A contains a splitting separable polynomial as $n - 2 \leq |K|$. Hence we may define p_A via $\langle p_A \rangle = P_A \cap P$ and $l_A \doteq \sum_{i=0}^{n-1} ([X_0^i X_1^{n-1-i}] p_A) e_i^*$. One derives that the hyperplanes $H_A := \ker l_A$ contain only the points $\mathrm{P}f(A)$ of $\mathcal{A}$ and intersect in a unique point $\hat{a}$ which extends $\mathcal{A}$. □

Furthermore, we want to prove that a normal rational curve is complete in more than half of the expected cases. For this we need the following elementary facts.

Lemma 4.6. *Let $Q \leq P_2$ be of codimension one. Then if Q is not of the form $Q = P_1 \det(X, \alpha)$ for some $\alpha \in \mathrm{P}K^2$ the following statements hold.*

(I) If $\operatorname{char} K = 2$*, then either* $Q = P_1^2$ *(i.e.* Q *consists entirely of squares) or* Q *contains one square,* $\frac{|K|}{2}$ *splitting separable polynomials and the same number of irreducible polynomials (up to scalar factor).*

(II) If $\operatorname{char} K \neq 2$*, then* Q *contains* 1 ± 1 *squares,* $\frac{|K| \mp 1}{2}$ *splitting separable polynomials and the same number of irreducible polynomials.*

Proof.

(I) If $\mathrm{P}Q$ contains two distinct squares, then it is clearly P_1^2 (since they already span a two-dimensional space). Otherwise, the kernel of the map $[X_0 X_1] : P_2 \to K$ intersects with Q in a one-dimensional space (showing that Q contains a square). The intersection of Q with $P_1 \det(X, \alpha)$ ($\alpha \in \mathrm{P}K^2$) is always of dimension one, since $Q \wedge P_1 \det(X, \alpha) < Q$ and $\dim(Q \wedge P_1 \det(X, \alpha)) = \dim Q + \dim(P_1 \det(X, \alpha)) - \dim(Q \vee P_1 \det(X, \alpha)) \geq 2 + 2 - 3$. Thus there are $\frac{|K|}{2}$ splitting separable polynomials in $\mathrm{P}Q$, one square and $\frac{|K|}{2}$ irreducible ones.

(II) Assume Q contains two squares. Choosing appropriate coordinates, we may assume that these are X_0^2 and X_1^2. But then any linear combination $\mu X_0^2 + \lambda X_1^2$ ($\lambda, \mu \in K^\times$) cannot be a square since then $\mu X_0^2 + \lambda X_1^2 = (\alpha X_0 + \beta X_1)^2 = \alpha^2 X_0^2 + 2\alpha\beta X_0 X_1 + \beta^2 X_1$ implying that $\alpha\beta = 0$ which leads to $\mu = 0$ or $\lambda = 0$. Moreover, if Q contains one square, say X_0^2, and is not of the form $P_1 \det(X, \alpha)$, then it contains a polynomial $aX_0^2 + bX_0X_1 + X_1^2$ which can be completed to a second square by adding $\left(\frac{b^2}{4} - a\right) X_0^2$.

Hence we are done. □

Remark 14. It is easy to see that for $K = \mathbb{F}_q$ and q even there exist exactly $q + 1$ subspaces of codimension one in P_2 of type $P_1 \det(X, \alpha)$, one subspace of type P_1^2 and $q^2 - 1$ subspaces containing only one square. When q is odd, there are $q + 1$ such subspaces of type $P_1 \det(X, \alpha)$ as well as $\binom{q+1}{2}$ subspaces with two squares and $\binom{q}{2}$ subspaces without square.

Lemma 4.7. *If a normal rational curve is incomplete in* PK^n *then* $\operatorname{char} K = 2$ *and* $n = 3$ *or*

$$\left\lceil \frac{|K| + 5}{2} \right\rceil \leq n.$$

Proof. If $n \geq |K| + 1$ we have already seen that no $|K| + 1$ arc is complete and embedded in an arc which is projectively equivalent to the arc $\{\langle e_0 \rangle, \ldots, \langle e_{n-1} \rangle, \langle e_0 + \cdots + e_{n-1} \rangle\}$ (cf. Corollary 3 (p. 7)). Thus assume $3 \leq n \leq |K|$, since for $n = 2$ the statement holds obviously (f is the identity map).

Let $\operatorname{char} K \neq 2$. Pick two $(n-2)$-sets $A, B \subseteq \mathrm{P}K^2$ such that $A \cap B = C$ is an $(n-3)$-set and the zeros z_A and z_B of order two of p_A and p_B are distinct (for this we need $2 \leq n - 1 \leq |K| + 1$,

e.g. we can then choose A first and then $B \subseteq \mathrm{P}K^2 \setminus \{z_A\}$). The space $\mathrm{P}\langle p_A, p_B\rangle$ contains exactly one polynomial with a set of zeros $C \cup \{c\}$ for all $c \in \mathrm{P}K^2 \setminus C$ — that is $|K| + 1 - (n-3)$ polynomials of this kind (the uniqueness follows from Lemma 4.5). Thus it contains exactly $|K| + 1 - (|K| + 1 - (n-3)) = n - 3$ polynomials which have exactly C as their zeros (the rest must be of that latter kind by Lemma 4.5). In the case where $\operatorname{char} K \neq 2$ we then immediately deduce that the space

$$\mathrm{P}\langle p_A/(p_A \wedge p_B), p_B/(p_A \wedge p_B)\rangle$$

contains 1 ± 1 squares, $\frac{|K|\mp 1}{2}$ splitting separable polynomials, and thus $\frac{|K|\mp 1}{2}$ irreducible polynomials. From this we get the inequality

$$\frac{|K| - 1}{2} \leq n - 3$$

since all irreducible polynomials p of the above space lead to a polynomial of the second kind by multiplying it by $\prod_{c\in C} \det(X, c)$. Thus

$$\frac{|K| + 5}{2} \leq n$$

if $\operatorname{char} K \neq 2$.

If $\operatorname{char} K = 2$ we need to pick A and B such that the cases $z_A = z_B$ and $\{z_A\} = A \setminus B$, $\{z_B\} = B \setminus A$ do not occur. So assume the second case occurs, then choose an $(n-2)$-set $D \subseteq \mathrm{P}K^2$ such that $D \cap B$ is an $(n-3)$-set which contains z_B (i.e. $D \cap B \neq C$; here we need that $4 \leq n$, since $1 \leq |\{z_B\}| \leq |D \cap B| = n - 3$). Define $A' := B$ and $B' := D$, then A' and B' cannot be of the second case by the choice of D. If these sets are of the first case, then p_B and p_D have the same zero of order two z_B and so $\langle p_B, p_D\rangle = P_1(p_B \wedge p_D)$ contains a polynomial $p_{B\cap D\cup\{z_A\}}$ (with the same zero of order two). $A'' := A$ and $B'' := B \cap D \cup \{z_A\}$ are sets avoiding the two bad cases since there double zeros are z_A and z_B (which are distinct by assumption) and $z_A \in B''$. Assuming that A and B are appropriately chosen it is simple to verify that the space $\mathrm{P}\langle p_A/(p_A \wedge p_B), p_B/(p_A \wedge p_B)\rangle$ (of homogeneous quadratic polynomials) contains one square, $\frac{|K|}{2}$ splitting separable polynomials and $\frac{|K|}{2}$ irreducible polynomials. This yields the inequality

$$\frac{|K|}{2} \leq n - 3, \text{ i.e. } \frac{|K| + 6}{2} \leq n,$$

completing the proof. □

The proof of this last fact seems to be simple, but although there are much better bounds for n — which I also rediscovered — it is not known to me, that the completeness of normal rational curves is established. We omit to present a proof of these other bounds since they are also not very satisfactory and the proof would be rather sophisticated.

4.2 Related matrices

Next, we discuss some interesting generator matrices of the MDS codes corresponding to a normal rational curve which seem natural to be mentioned at this point.

Extended VANDERMONDE matrices. Denote the elements of $\mathbb{F}_q$ by ν_i $(i = 0, \ldots, q-1)$ and define a representation V of a normal rational curve as given in Definition 4.1 (p. 17) by

$$V \coloneqq \left\{ \begin{pmatrix} 1 \\ \nu_i \\ \vdots \\ \nu_i^{n-1} \end{pmatrix} : i = 0, \ldots, n-1 \right\} \cup \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \right\}$$

and a check matrix (by writing down the vectors of the above representation in a 'natural order')

$$G_V \coloneqq \begin{pmatrix} 1 & \cdots & 1 & 0 \\ \nu_0 & \cdots & \nu_{q-1} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ \nu_0^n & \cdots & \nu_{q-1}^n & 1 \end{pmatrix}.$$

One then checks easily that G_V has the property that any n distinct column vectors are linearly independent since any submatrix

$$U \coloneqq \begin{pmatrix} 1 & \cdots & 1 \\ \nu_{k_1} & \cdots & \nu_{k_n} \\ \vdots & \ddots & \vdots \\ \nu_{k_1}^{n-1} & \cdots & \nu_{k_n}^{n-1} \end{pmatrix}$$

is a VANDERMONDE *matrix* in the case it does not contain the last vector having determinant

$$\det U = \prod_{i<j} (\nu_{k_i} - \nu_{k_j})$$

which is not zero as all ν_k are distinct. In the other case, the determinant is also non-zero, as one notes by applying LAPLACE's formula to the last column. Actually, it is immediately clear that any n column vectors of the above matrix are linearly independent by Lemma 4.1 (p. 17) but we just wanted to point out another way to see this.

The representation V of a classical arc introduced in this section is called VANDERMONDE *representation* and G_V is called extended VANDERMONDE matrix in the sequence of elements $(\nu_0, \ldots, \nu_{q-1})$. It is a generator matrix of the *extended* REED-SOLOMON *code*[5]

Extended CAUCHY matrices. In the last paragraph we saw that the arcs corresponding to extended REED-SOLOMON codes are precisely normal rational curves. We want to construct another type of generator matrix from a normal rational curve (so that the corresponding code will be ${\mathbb{F}_q}^\times \wr S_n$-equivalent to the extended REED-SOLOMON code). The first step is to realize that

$$C' \coloneqq \left\{ \begin{pmatrix} P_0(z) \\ \vdots \\ P_{n-1}(z) \end{pmatrix} \in \mathbb{F}_q^n : z \in \mathbb{F}_q \right\} \cup \left\{ \begin{pmatrix} p_0^{n-1} \\ \vdots \\ p_{n-1}^{n-1} \end{pmatrix} \right\}$$

[5]Basically, there are many possibilities to introduce REED-SOLOMON codes and mostly the definitions do coincide only up to ${\mathbb{F}_q}^\times \wr S_m$-equivalence where m is the length of the code — here $m = |K| + 1$.

is a representation of a normal rational curve (since it is obviously PGL-equivalent to the 'one' given in Definition 4.1 (p. 17) by the mapping f) where $P_i = \sum_{j=0}^{n-1} p_i^j X^j$ $(i = 0, \ldots, n-1)$ form a basis of the polynomials of degree $k \leq n-1$. Now we pick the first n distinct elements $\nu_0, \ldots, \nu_{n-1} \in \mathbb{F}_q$ and set

$$P_i := \prod_{\substack{j=0 \\ j \neq i}}^{n-1} (X - \nu_j) \in \mathbb{F}_q[X].$$

It is then immediately clear that the P_i are linearly independent, since $\frac{1}{\prod_{j \neq i}(\nu_i - \nu_j)} P_i$ form a LAGRANGE basis with respect to the points ν_i $(i = 0, \ldots, n-1)$. The point $\langle e_\infty \rangle$ corresponding to the preimage ∞ now evaluates to

$$e_\infty = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \sum_{i=0}^{n-1} e_i.$$

To abbreviate notation we also set

$$P(z) := \begin{pmatrix} P_0(z) \\ \vdots \\ P_{n-1}(z) \end{pmatrix}.$$

Starting from the representation C' and scaling all vectors $P(\nu_i)$ of the representation $(i = 0, \ldots, n-1)$ by

$$\prod_{\substack{j=0 \\ j \neq i}}^{n-1} \frac{1}{\nu_i - \nu_j},$$

the vectors $P(\nu_i)$ $(i = n, \ldots, q-1)$ by

$$\prod_{j=0}^{n-1} \frac{1}{\nu_i - \nu_j}$$

and leaving $e_\infty = \sum_{i=0}^{n-1} e_i$ fixed we get a representation

$$C = \left\{ e_1, \ldots, e_n, \sum_{i=1}^{n} e_i \right\} \cup \left\{ \begin{pmatrix} \frac{1}{\nu_i - \nu_0} \\ \vdots \\ \frac{1}{\nu_i - \nu_{n-1}} \end{pmatrix} : i = n, \ldots, q-1 \right\}$$

of a curve being PGL-equivalent to the initial curve. However, writing down the generator matrix of the corresponding MDS code (in a 'natural order') we obtain

$$G_C = \begin{pmatrix} 1 & 0 & \cdots & 0 & 1 & \frac{1}{\nu_n - \nu_0} & \cdots & \frac{1}{\nu_{q-1} - \nu_0} \\ 0 & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 1 & \frac{1}{\nu_n - \nu_{n-1}} & \cdots & \frac{1}{\nu_{q-1} - \nu_{n-1}} \end{pmatrix}$$

which contains a CAUCHY *matrix*. Hence, we call the representation C of a classical arc the CAUCHY *representation*. The matrix consisting of the columns of index n till q (starting from zero) is called *extended* CAUCHY *matrix* in the sequences $(\nu_0, \ldots, \nu_{n-1})$ and $(\nu_n, \ldots, \nu_{q-1})$ (which is a totally regular matrix).

5 The proof of the MDS main conjecture for $n \leq 2p-2$

In the following we aim to present the results of the two papers [1] and [3] simplifying some aspects of the proofs.

5.1 SEGRE's lemma of tangents

Any attempt to answer the MDS main conjecture uses a lemma which was first stated by B. SEGRE and can be considered as a key result. To state it we need the following

Definition 5.1 (tangent polynomials). Let $\mathcal{A}$ be an arc in $\mathbb{F}_q^n$. Then for any $(n-2)$-set $X \subseteq \mathcal{A}$ define the tangent polynomial T_X as the product

$$T_X \doteq \prod_{\substack{H \in \operatorname{Sub} \mathbb{F}_q^n \\ \operatorname{codim} H = 1 \\ H \cap \mathcal{A} = X}} l_H$$

where l_H are linear forms such that $\ker l_H = H$. This defines (up to scalar factor from ${\mathbb{F}_q}^\times$) a homogeneous polynomial in n variables which is of degree $q+1-(\mathcal{A}-(n-2)) = q-1+n-|\mathcal{A}| =: t$ (by counting the corresponding hyperplanes).

The main idea of this section is to present a way to choose the tangent polynomials canonically with respect to a given order on the elements of the arc. This will simplify the calculation in the proofs of various lemmas a lot.

Remark 15. From $t \geq 0$ one gets the weak bound $|\mathcal{A}| \leq q+n-1$ which we already derived in Section 3 (p. 13).

Now we are able to state the lemma.

Lemma 5.1 (SEGRE's lemma of tangents, original version). *Let $n \geq 3$ and $\mathcal{A}$ be a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$. Then for pairwise distinct $x_i \in \mathcal{A}$ $(i = 0, 1, 2)$ and $X \subseteq \mathcal{A} \setminus \{x_0, x_1, x_2\}$, $|X| = n-3$ we have*

$$\frac{T_{X\cup\{x_0\}}(x_1) T_{X\cup\{x_1\}}(x_2) T_{X\cup\{x_2\}}(x_0)}{T_{X\cup\{x_1\}}(x_0) T_{X\cup\{x_2\}}(x_1) T_{X\cup\{x_0\}}(x_2)} = (-1)^{t+1}.$$

Remark 16. The expression in the lemma is well-defined since the scalar factors in T_Y vanish in the fraction.

Proof. Denote by x_i^* the linear form corresponding to x_i in the dual basis of $X' \coloneqq X \cup \{x_0, x_1, x_2\}$. For $i \in \{0,1,2\}$ let $\mathcal{H}_i$ be the set of hyperplanes H containing $\langle X, x_i\rangle$ but not x_j for $j \neq i$. For each hyperplane $H \in \mathcal{H}_i$ there are two possibilities:

Case 1. There is an $a \in \mathcal{A} \setminus X'$ with $a \in H$. In this case define the linear form

$$l_H \coloneqq \det(\bullet, x_i, X, a)$$

Case 2. Otherwise, l_H is already defined via the tangent polynomials. Now, one may define the polynomial $P_i \coloneqq \prod_{H\in\mathcal{H}_i} l_H$ (of degree $q-1$) and one computes that

$$P_i(x_j) = T_{X\cup\{x_i\}}(x_j) \prod_{a\in\mathcal{A}\setminus X'} \det(x_j, x_i, X, a).$$

When $\{0,1,2\} \setminus \{i\} = \{j,k\}$ it is clear that $P_i(x_j)/P_i(x_k) = -1$ which can be deduced from the fact that the product of all units of a finite field is -1 and the observation that all hyperplanes in $\mathcal{H}_i$ are given by $\ker(x_j^* + \lambda x_k^*)$ where $\lambda \in {\mathbb{F}_q}^\times$. Thus we have

$$\begin{aligned}\frac{P_1(x_1)P_2(x_2)P_3(x_0)}{P_2(x_0)P_3(x_1)P_1(x_2)} &= \frac{T_{X\cup\{x_0\}}(x_1)T_{X\cup\{x_1\}}(x_2)T_{X\cup\{x_2\}}(x_0)}{T_{X\cup\{x_1\}}(x_0)T_{X\cup\{x_2\}}(x_1)T_{X\cup\{x_0\}}(x_2)} \\ &\quad\times \prod_{\substack{i,j\in\{0,1,2\}\\ i<j}} \prod_{a\in\mathcal{A}\setminus X'} \frac{\det(x_i, x_j, X, a)}{\det(x_j, x_i, X, a)} \\ &= (-1)^3 = -1.\end{aligned}$$

Since $\mathcal{A} \setminus X'$ has $|\mathcal{A}| - n = q - 1 - t$ elements, the last two products evaluate to $(-1)^{3(q-1-t)} = (-1)^t$. This finishes the proof. □

For convenience we now state a 'simplified version' of SEGRE's lemma which is the only version we shall use in the following.

At first it becomes necessary to recall the meaning of the following notation from the preliminaries.

Convention 5.1 (sequence notation). By $(A_0, \ldots, A_{m-1})$ we mean the sequence as explained in Preliminaries (p. iv) where A_i is a subset of some ordered set A.

Corollary 5 (Simplification of SEGRE's lemma). Let $\mathcal{A}$ be a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$ ($n \geq 3$) and $\leq$ some linear order on $\mathcal{A}$. Then we can define the tangent polynomials T_Y ($Y \subseteq \mathcal{A}$, $|Y| = n-2$) such that for all x_0, x_1, X we have

$$\frac{T_{X\cup\{x_1\}}(x_0)}{T_{X\cup\{x_0\}}(x_1)} = \left(\frac{\operatorname{sgn}(X \cup \{x_1\}, x_0)}{\operatorname{sgn}(X \cup \{x_0\}, x_1)}\right)^{t+1}$$

where $X \subseteq \mathcal{A}$ has $n-3$ elements and $x_0, x_1 \in \mathcal{A} \setminus X$ are distinct.

Proof. We define the directed graph $G = (V, E)$ by $V := \binom{\mathcal{A}}{n-2}$ and $E := \{(u, v) \in V^2 : |u \setminus v| = 1\}$. Moreover, we define a labeling $\lambda : E \to {\mathbb{F}_q}^\times$. For $(u, v) \in E$ let $u_v \in u \setminus v$ and $v_u \in v \setminus u$ be the elements of the singletons. Then define

$$\lambda(u, v) := \frac{T_u(v_u)}{T_v(u_v)}.$$

For the two types of triangles in G we have two different relations holding. A triangle of the first type consists of vertices $u, v, w \in V$ such that $|u \cup v \cup w| = n - 1$. Here it clearly holds that

$$\lambda(u, v)\lambda(v, w)\lambda(w, u) = \frac{T_u(v_u)T_v(w_v)T_w(u_w)}{T_v(u_v)T_w(v_w)T_u(w_u)} = 1$$

which is a trivial equation since $v_u = w_u$, $u_v = w_v$, $u_w = v_w$. For a triangle of the second type consisting of vertices $u, v, w \in V$ such that $|u \cup v \cup w| = n$ we obtain

$$\lambda(u, v)\lambda(v, w)\lambda(w, u) = (-1)^{t+1}$$

by Lemma 5.1 (p. 24) where $X := u \cap v \cap w$ and $x_0 := u_v = u_w$, $x_1 := v_u = v_w$, $x_2 := w_u = w_v$. It is thus clear, that λ is uniquely defined by any restriction $\lambda|_{E_T}$ where $T = (V, E_T)$ is a (directed) rooted spanning tree of G with root $r \in V$ (by the above relations in triangles of G and as G is obviously strongly connected). Moreover, when replacing T_u by $T'_u := \mu T_u$ one just modifies λ to λ' where

$$\lambda'(v, w) = \begin{cases} \lambda(v, w) & : u \notin \{v, w\} \\ \mu\lambda(v, w) & : v = u \\ \mu^{-1}\lambda(v, w) & : w = u \end{cases}.$$

This idea can be used to modify the tangent polynomials step by step to achieve any values of λ among E_T. Define the sets $V_l := \{v \in V : d_T(r, v) = l\}$ ($l \in \mathbb{N}$, here $d_T(\bullet_1, \bullet_2)$ means the metric of the shortest path on T). Since G is finite there is some $L \in \mathbb{N}$ such that $\{V_l : l = 0, \ldots, L\}$ is a partition of V. Moreover, one notes that the sets $E_l := \{(u, v) \in E_T : u \in V_{l-1}, v \in V_l\}$ for $l = 1, \ldots, L$ form a partition of E_T. Thus one can modify the labeling λ at first on E_1 then on E_2 etc. As there is no edge in T between the sets V_m and V_n where $|n - m| \geq 2$ this procedure works and one does not destroy former changes on some E_i. This shows that λ can be changed to any labeling satisfying the two triangle conditions. Lastly, we check that these are satisfied for the labeling $\overline{\lambda}$ given in the lemma, where for $(u, v) \in E$

$$\overline{\lambda}(u, v) := \left(\frac{\operatorname{sgn}(u, v_u)}{\operatorname{sgn}(v, u_v)}\right)^{t+1}.$$

For a triangle uvw of the first type ($|u \cup v \cup w| = n - 1$) we obtain $v_u = w_u$, $u_v = w_v$, $u_w = v_w$ and thus one gets

$$\overline{\lambda}(u, v)\overline{\lambda}(v, w)\overline{\lambda}(w, u) = \left(\frac{\operatorname{sgn}(u, v_u)}{\operatorname{sgn}(v, u_v)}\frac{\operatorname{sgn}(v, w_v)}{\operatorname{sgn}(w, v_w)}\frac{\operatorname{sgn}(w, u_w)}{\operatorname{sgn}(u, w_u)}\right)^{t+1} = 1$$

Similarly, for a triangle uvw of the second type ($|u \cup v \cup w| = n$) one gets the desired identity by the following reasoning. W.l.o.g. we may write $u = X \cup \{x_0\}$, $v = X \cup \{x_1\}$, $w = X \cup \{x_2\}$ for an

$(n-3)$-element set $X \coloneqq u \cap v \cap w$ and elements $x_i \in \mathcal{A}$ $(i = 0, 1, 2)$ such that $\{x_0, x_1, x_2\} \cup X = u \cup v \cup w$. Furthermore, we may assume that $X_0 < x_0 < X_1 < x_1 < X_2 < x_2 < X_3$, where X_0, X_1, X_2, X_3 partitions X (otherwise interchange the labeling of u, v and w; some sets X_i may of course be empty for $i = 0, \ldots, 3$). Then compute

$$\begin{aligned}
\overline{\lambda}(u,v)\overline{\lambda}(v,w)\overline{\lambda}(w,u) &= \left(\frac{\operatorname{sgn}(X_0, x_0, X_1, X_2, X_3, x_1)}{\operatorname{sgn}(X_0, X_1, x_1, X_2, X_3, x_0)}\right)^{t+1} \\
&\quad \times \left(\frac{\operatorname{sgn}(X_0, X_1, x_1, X_2, X_3, x_2)}{\operatorname{sgn}(X_0, X_1, X_2, x_2, X_3, x_1)}\right)^{t+1} \\
&\quad \times \left(\frac{\operatorname{sgn}(X_0, X_1, X_2, x_2, X_3, x_0)}{\operatorname{sgn}(X_0, x_0, X_1, X_2, X_3, x_2)}\right)^{t+1} \\
&= (-1)^{((|X_2|+|X_3|)+(|X_1|+1+|X_2|+|X_3|))(t+1)} \\
&\quad \times (-1)^{(|X_3|+(|X_2|+1+|X_3|))(t+1)} \\
&\quad \times (-1)^{((|X_1|+|X_2|+1+|X_3|)+|X_3|)(t+1)} \\
&= (-1)^{t+1}
\end{aligned}$$

to end the proof. □

This lemma enables us to make the following definition.

Definition 5.2. Let $\mathcal{A} \subseteq \mathbb{F}_q^n$ be a representation of an arc. We say that its tangent polynomials are defined canonically with respect to the linear order $\leq$ on $\mathcal{A}$ if they satisfy for all x_0, x_1, X the identity

$$\frac{T_{X\cup\{x_1\}}(x_0)}{T_{X\cup\{x_0\}}(x_1)} = \left(\frac{\operatorname{sgn}(X \cup \{x_1\}, x_0)}{\operatorname{sgn}(X \cup \{x_0\}, x_1)}\right)^{t+1}$$

where $X \subseteq \mathcal{A}$ has $n-3$ elements and $x_0, x_1 \in \mathcal{A} \setminus X$ are distinct.

This simple but effective trick enables us to prove some results of BALL and DE BEULE avoiding the occurrence of some inconvenient terms in the calculation. Note that in the above definition the tangent polynomials are still only defined up to scalar factor, but their quotients are fixed. In the following we do only work with the tangent polynomials chosen in that manner.

Actually, we shall use new symbols $P(X)$ for the evaluation of tangent polynomials in subsequent calculations.

Definition 5.3 (abbreviation of tangent polynomial evaluations). Let $\mathcal{A}$ be a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$ such that the tangent polynomials T_Y are defined canonically with respect to some linear order $\leq$ on $\mathcal{A}$. Then we set $P(X) \coloneqq T_{X\setminus\{x\}}(x)$ where x is the biggest element in X.

6 Interpolation formulae

An elementary but particularly nice idea is to use interpolation to capture information about the arc.

There are two basic possibilities to apply interpolation.

Lemma 6.1 (interpolation of the tangent polynomial). *Let $\mathcal{A} \subseteq \mathbb{F}_q^n$ be a representation of an arc and $A, B \subseteq \mathcal{A}$ be disjoint subsets with $|A| = t + 2$ and $|B| = n - 2$. Then*

$$\sum_{a \in A} T_B(a) \prod_{z \in A \setminus \{a\}} \det(z, B, a)^{-1} = 0$$

holds or equivalently, when the tangent polynomials are defined canonically with respect to some linear order $\leq$,

$$\sum_{a \in A} P(\{a\} \cup B) \prod_{z \in A \setminus \{a\}} \det(z, \{a\} \cup B)^{-1} = 0.$$

Proof. As $T_B(x + y) = T_B(x)$ for all $x \in \mathbb{F}_q^n$ and $y \in \langle B \rangle$ we may interpolate the polynomial $\overline{T}_B(x + \langle B \rangle) \coloneqq T_B(x)$ as a homogeneous polynomial of degree t over $\mathbb{F}_q^n / \langle B \rangle$. To do this, pick $a \in A$ to get

$$T_B(x) = \sum_{a' \in A \setminus \{a\}} T_B(a') \prod_{z \in A \setminus \{a, a'\}} \frac{\det(z, B, x)}{\det(z, B, a')},$$

since both sides are polynomials in x of degree t and both are constant on cosets of $\langle B \rangle$ and agree on $t + 1$ points of $\mathbb{F}_q^n / \langle B \rangle$ (namely $a' + \langle B \rangle$ for $a' \in A \setminus \{a\}$), for which the right hand side is a LAGRANGE interpolation formula. Replacing x by a and dividing by $\prod_{z \in A \setminus \{a\}} \det(z, B, a)$ one gets

$$T_B(a) \prod_{z \in A \setminus \{a\}} \det(z, B, a)^{-1} = \det(a', B, a)^{-1} \sum_{a' \in A \setminus \{a\}} T_B(a') \prod_{z \in A \setminus \{a, a'\}} \det(z, B, a')^{-1}$$

which is what we wanted to prove. The second formulation in the lemma follows from the fact that the tangent polynomials are defined canonically with respect to an underlying linear order and the definition of $P(X)$ together with Corollary 5 (p. 25). □

Another idea is to interpolate the determinants themselves.

Lemma 6.2 (interpolation of determinants). *Let $A, B, C \subseteq \mathbb{F}_q^n$ such that $\langle A \cup C \rangle = \mathbb{F}_q^n$, $|A| + |C| = n + 1$ and $|B| + |C| = n - 1$, and let $\leq$ be some linear order on $A \cup B \cup C$. Then we have*

$$\sum_{a \in A} \operatorname{sgn}(a, A \setminus \{a\} \cup C) \det(a, B \cup C) \det(A \setminus \{a\} \cup C) = 0.$$

Here, sgn *is taken with respect to $\leq$.*

Proof. Picking $a \in A$ and interpolating $\det(\bullet, B \cup C)$ as a linear form in $\mathbb{F}_q^n / \langle C \rangle$ gives

$$\det(x, B \cup C) = \sum_{a' \in A \setminus \{a\}} \det(a', B \cup C) \frac{\det(x, A \setminus \{a, a'\} \cup C)}{\det(a', A \setminus \{a, a'\} \cup C)}$$

which holds as it holds for $x \in A \setminus \{a\} \cup C$ which is a basis of $\mathbb{F}_q^n$. Replacing x by a and rearranging the terms yields

$$\begin{aligned}
\det(a, B \cup C) \det(A \setminus \{a\} \cup C) &= \sum_{a' \in A \setminus \{a\}} \det(a', B \cup C) \frac{\det(a, A \setminus \{a, a'\} \cup C)}{\operatorname{sgn}(a', A \setminus \{a, a'\} \cup C)} \\
&= \sum_{a' \in A \setminus \{a\}} \det(a', B \cup C) \det(A \setminus \{a'\} \cup C) \frac{\operatorname{sgn}(a, A \setminus \{a, a'\} \cup C)}{\operatorname{sgn}(a', A \setminus \{a, a'\} \cup C)} \\
&= - \sum_{a' \in A \setminus \{a\}} \det(a', B \cup C) \det(A \setminus \{a'\} \cup C) \frac{\operatorname{sgn}(a', A \setminus \{a'\} \cup C)}{\operatorname{sgn}(a, A \setminus \{a\} \cup C)},
\end{aligned}$$

which is the desired result. □

6.1 Manipulation of interpolation identities

General assumptions. For the rest of this section we fix $\mathcal{A} \subseteq \mathbb{F}_q^n$ as a representation of an arc in $\mathrm{P}\mathbb{F}_q^n$ with a linear order $\leq$ explained on it, $P(X)$ as the evaluations of tangent polynomials of $\mathcal{A}$ as defined in Definition 5.3 (p. 27), $p = \operatorname{char} \mathbb{F}_q$ as the characteristic of the finite field $\mathbb{F}_q$ and $t \coloneqq q + n - 1 - |\mathcal{A}|$ as the degree of the tangent polynomials of $\mathcal{A}$.

Now, the idea is to play with the interpolation identities to reach a contradiction in the case where $t \leq n - 3$ (i.e. $|\mathcal{A}| \geq q + 2$).

First attempt. The proof of the main conjecture for MDS codes of Ball and de Beule for the case in which $n \leq p$ and the classification of $(q+1)$-arcs in that case is based on the following key result which can be derived by elementary means from the interpolation of tangent polynomials.

Lemma 6.3 (Ball & de Beule's *ABC* lemma). *Let $0 \leq r \leq \min\{n, p\} - 1$ and $A, B, C \subseteq \mathcal{A}$ disjoint sets such that $|A| + |B| = r + t + 1$, $|C| = n - 1 - r$. We then have*

$$\begin{aligned}
&(-1)^r \sum_{\substack{A' \subseteq A \\ |A'| = r}} P(A' \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup C)^{-1} \\
&= \sum_{\substack{B' \subseteq B \\ |B'| = r}} P(B' \cup C) \prod_{z \in (B \setminus B') \cup A} \det(z, B' \cup C)^{-1}.
\end{aligned}$$

Proof. The proof happens by induction on r. For $r = 0$ the statement is a trivial. Now, suppose the lemma is proven for $r - 1 \geq 0$ and let $r \leq \min\{n, p\} - 1$. Moreover, let $A, B, C \subseteq \mathcal{A}$ be disjoint sets such that $|A| + |B| = r + t + 1$, $|C| = n - 1 - r$. Then pick $a \in A$ and apply the lemma for $r - 1$ and sets $A \setminus \{a\}$, B, $\{a\} \cup C$ (if A and B are empty the lemma is obvious — moreover, the roles of A and B are symmetric). This yields

$$\begin{aligned}(-1)^{r-1} \sum_{\substack{A' \subseteq A \setminus \{a\} \\ |A'| = r-1}} P(A' \cup \{a\} \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup \{a\} \cup C)^{-1} \\ = \sum_{\substack{B' \subseteq B \\ |B'| = r-1}} P(B' \cup \{a\} \cup C) \prod_{z \in (B \setminus B') \cup A \setminus \{a\}} \det(z, B' \cup \{a\} \cup C)^{-1}.\end{aligned}$$

Summing over $a \in A$ gives

$$\begin{aligned}&(-1)^{r-1} r \sum_{\substack{A' \subseteq A \\ |A'| = r}} P(A' \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup C)^{-1} \\ &= \sum_{\substack{B' \subseteq B \\ |B'| = r-1}} \sum_{a \in A} P(B' \cup \{a\} \cup C) \prod_{z \in (B \setminus B') \cup A \setminus \{a\}} \det(z, B' \cup \{a\} \cup C)^{-1} \\ &= \sum_{\substack{B' \subseteq B \\ |B'| = r-1}} \sum_{a \in A} P(B' \cup \{a\} \cup C) \prod_{z \in (B \setminus B' \cup A) \setminus \{a\}} \det(z, B' \cup \{a\} \cup C)^{-1} \\ &= - \sum_{\substack{B' \subseteq B \\ |B'| = r-1}} \sum_{b \in B \setminus B'} P(B' \cup \{b\} \cup C) \prod_{z \in (B \setminus B' \cup A) \setminus \{b\}} \det(z, B' \cup \{b\} \cup C)^{-1} \\ &= -r \sum_{\substack{B' \subseteq B \\ |B'| = r}} P(B' \cup C) \prod_{z \in (B \setminus B') \cup A} \det(z, B' \cup C)^{-1}.\end{aligned}$$

Here we used the interpolation of tangent polynomials in the fourth line for the sets $B' \cup C$ and $B \setminus B' \cup A$ when $r - 1 \leq |B|$. In the case $|B| < r - 1$ the left hand side is zero (as it had been zero before). If $r \leq p - 1$ it is a unit and we can divide the above by $-r$ to complete the induction. □

We thus immediately obtain

Corollary 6 (the case $n \leq p$). If $n \leq p$ then $|\mathcal{A}| \leq q + 1$.

Proof. Assume that $n \leq p$ and $|\mathcal{A}| \geq q + 2$ or equivalently $t = q + n - 1 - |\mathcal{A}| \leq n - 3$. Then apply Lemma 6.3 with $r = |A| = n - 1 \leq p - 1$ and appropriate subsets B, C (as $\min\{n, |\mathcal{A}| - n\} \leq |\mathcal{A}|/2$, using the dual arc (cf. Definition 2.2 (p. 6)) if necessary we may assume w.l.o.g. that $n + t \leq 2n - 3 \leq |\mathcal{A}|$). We have $|B| = t + 1 \leq n - 2$ and thus the lemma gives

$$(-1)^{n-1} P(A) \prod_{z \in B} \det(z, A)^{-1} = 0$$

which is a contradiction. □

Remark 17. This is as we will see the optimal result using *only* the interpolation of the tangent polynomial in the sense that the corresponding system of equations for $t = n - 3$ is regular if and only if $n \leq p$ (cf. Section 7).

Moreover, in that case the $(q+1)$-arcs can be identified as normal rational curves.

Corollary 7 (classification of $(q+1)$-arcs for $n \leq p$). Let $n \leq p$. Then $\mathcal{A}$ is a normal rational curve.

Proof. In the case $|\mathcal{A}| = q + 1$ one has $t = n - 2$. Again, we apply Lemma 6.3 (p. 29) for $r = n-1 \leq p-1$ and $A \subseteq \mathcal{A}$ with $|A| = n$ and appropriate sets $B, C \subseteq \mathcal{A}$ (here $|B| = t = n-2 < r$ and $C = \emptyset$). This gives

$$(-1)^{n-1} \sum_{\substack{A' \subseteq A \\ |A'|=n-1}} P(A') \prod_{z \in (A \setminus A') \cup B} \det(z, A')^{-1} = 0.$$

Applying the above for A and $B_b \coloneqq B \setminus \{b\} \cup \{x\}$ for some fixed point $x \in \mathcal{A} \setminus A$ we obtain the $n - 2$ equations

$$\sum_{a \in A} P(A \setminus \{a\}) \prod_{z \in B} \det(z, A \setminus \{a\})^{-1} \frac{\det(b, A \setminus \{a\})}{\det(a, A \setminus \{a\})} \det(x, A \setminus \{a\})^{-1} = 0 \quad (b \in B). \tag{1}$$

We could also have written $a^*(b)$ (where a^* means an element of the dual basis of A) for the fraction of determinants showing that the matrix $M \in \mathbb{F}_q^{B \times A}$ defined by

$$M \coloneqq (m_{ba})_{(b,a) \in B \times A}, \quad m_{ba} \coloneqq \frac{\det(b, A \setminus \{a\})}{\det(a, A \setminus \{a\})}$$

has full rank as its rows are just the coordinate vectors of each $b \in B$ with respect to the basis A. Thus it follows that the matrix $N \coloneqq MD$, where

$$D \coloneqq \operatorname{diag}\left(P(A \setminus \{a\}) \prod_{z \in \{a\} \cup B} \det(z, A \setminus \{a\})^{-1} : a \in A \right),$$

has full rank which is the matrix of the linear system (1) in

$$\left(\frac{\det(a, A \setminus \{a\})}{\det(x, A \setminus \{a\})} \right)_{a \in A}.$$

Hence the kernel of this system has dimension $|A| - |B| = n - (n - 2) = 2$ showing that the image of x for all $x \in \mathcal{A} \setminus A$ under the map

$$\gamma : (\mathbb{F}_q{}^{\times})^n \to (\mathbb{F}_q{}^{\times})^n$$

where $(\mathbb{F}_q{}^\times)^n \coloneqq \mathbb{F}_q^n \setminus \bigcup_{a\in A} \langle A\setminus\{a\}\rangle$ and

$$\sum_{a\in A}\lambda_a a \mapsto \sum_{a\in A}\lambda_a^{-1}a$$

must lie on a (projective) line i.e. in a two dimensional subspace of $\mathbb{F}_q^n$. Using an appropriate element of $M \in \mathrm{PGL}(n,\mathbb{F}_q)$ which maps $\langle a\rangle \mapsto \langle a\rangle$ for $a\in A$ and $\langle\hat{x}\rangle \mapsto \left\langle\sum_{a\in A} a\right\rangle$ for some $\hat{x}\in\mathcal{A}\setminus A$ we may assume w.l.o.g. that $\hat{a} \coloneqq \sum_{a\in A} a \in \mathcal{A}$. Set $\hat{A} \coloneqq A\cup\{\hat{a}\}$.

Rescaling $\gamma(x)$ ($x\in\mathcal{A}\setminus\hat{A}$) appropriately we obtain scalars α_x such that

$$\alpha_x\gamma(x) = \check{a} - \hat{a}\lambda_x$$

lie on an affine line parallel to $\langle\hat{a}\rangle$ in $\mathbb{F}_q^n$ (for some $\check{a}\in\mathbb{F}_q^n$ and $\lambda_x\in\mathbb{F}_q$). This is possible since the point $\langle\hat{a}\rangle$ lies on the same projective line as all $\langle x\rangle\in\mathcal{A}\setminus\hat{A}$ so the latter lie in an affine line parallel to $\langle\hat{a}\rangle$. Changing the parameters if necessary by a translation $x\mapsto x+\mu$ ($\mu\in\mathbb{F}_q$), we may assume that $0=\lambda_x$ for some $x\in\mathcal{A}\setminus\hat{A}$ whence $\check{a}\in(\mathbb{F}_q{}^\times)^n$.

The line $\lambda\mapsto\check{a}-\hat{a}\lambda$ intersects the n hyperplanes $\langle A\setminus\{a\}\rangle$ (for $a\in A$) in n distinct points (i.e. in the coordinate representation $\check{a}=\sum_{a\in A}\nu_a a$ all ν_a are distinct for $a\in A$). This holds as the assumption $\nu_{a'}=\nu_{a''}$ for $a',a''\in A$, $a'\neq a''$ leads to the contradiction $\{\hat{a},\check{a}\}\cup A\setminus\{a',a''\}\subseteq\mathcal{A}$ forming a linearly dependent n-set.

Therefore, we may deduce that

$$\{\nu_a : a\in A\}\cup\left\{\lambda_x : x\in\mathcal{A}\setminus\hat{A}\right\} = \mathbb{F}_q$$

is a disjoint union as all $\check{a}-\hat{a}\lambda_x$ have no coordinates equal to zero in the basis A. However, considering the set $\hat{\mathcal{A}}\coloneqq\hat{A}\cup\left\{\gamma^{-1}\circ\alpha_x\circ\gamma(x) : x\in\mathcal{A}\setminus\hat{A}\right\}$ we have a representation of the same arc which is a Cauchy-representation shown in 4.2 (p. 23). So the arc represented by $\mathcal{A}$ is a normal rational curve. □

Remark 18. The argument can also be used to prove that the cardinality of an arc in $\mathrm{P}\mathbb{F}_q^n$ ($n\le p$) can at most become $q+1$ (similarly to Corollary 6 (p. 30)).

Second attempt. In this paragraph we prove the same result for $n\le 2p-2$ and will bring in the interpolation of determinants. A classification of $(q+1)$-arcs is not given.

Lemma 6.4 (Ball's & de Beule's *ABCDE* lemma). *Let $n>p$ and $0<r\le p-1$ and $0\le m\le\min\{n-1-r,t+2\}$. Moreover, let A, B, C, D and E be disjoint subsets of $\mathcal{A}$ with $|A|=|B|=m$, $|C|=t+2-m$, $|D|=n-1-r-m$, $|E|=r-1$ and let there be given bijections $m\to A$ and $m\to B$ such that A_τ, B_τ denote the images of $\tau\subseteq m=\{0,\dots,m-1\}$. Then we have*

$$0 = \sum_{\substack{C'\subseteq C\\|C'|=r}}\sum_{\tau\subseteq m}(-1)^{|\tau|}P(A_\tau\cup B_{m\setminus\tau}\cup C'\cup D) \times\prod_{\substack{z\in A_{m\setminus\tau}\cup B_\tau\\\cup(C\setminus C')\cup E}}\det(z,A_\tau\cup B_{m\setminus\tau}\cup C'\cup D)^{-1}.$$

Proof. The proof happens by induction on m. We have $n > p$ so we may apply the Lemma 6.3 (p. 29) for $r \leq p-1$ and sets A, B, C with $|A| = t+2$, $|B| = r-1$ and $|C| = n-1-r > 0$. This gives

$$0 = \sum_{\substack{A' \subseteq A \\ |A'|=r}} P(A' \cup C) \prod_{z \in (A \setminus A') \cup B} \det(z, A' \cup C)^{-1}.$$

proving the lemma for $m = 0$ when replacing A by C, B by E and C by D.

For the induction step, assume the lemma holds for $m-1$ and for given A, B, C, D and E with $|A| = |B| = m$, $|C| = t+2-m$, $|D| = n-1-r-m$, $|E| = r-1$ pick $a := a_m \in A$ and $b := b_m \in B$ and apply the induction hypothesis for $\overline{A} := A \setminus \{a\}$, $\overline{B} := B \setminus \{b\}$, $C \cup \{a\}$, $D \cup \{b\}$, E and $\overline{A}$, $\overline{B}$, $C \cup \{b\}$, $D \cup \{a\}$, E (and $m-1$), respectively. This yields (the terms where $a \in C'$ on the left hand side and $b \in C'$ on the right hand side cancel out)

$$\begin{aligned}
&\sum_{\substack{C' \subseteq C \\ |C'|=r}} \sum_{\tau \subseteq m-1} (-1)^{|\tau|} P(\overline{A}_\tau \cup \overline{B}_{(m-1)\setminus\tau} \cup \{b\} \cup C' \cup D) \\
&\quad \times \prod_{\substack{z \in \overline{A}_{(m-1)\setminus\tau} \cup \{a\} \cup \overline{B}_\tau \\ \cup (C \setminus C') \cup E}} \det(z, \overline{A}_\tau \cup \overline{B}_{(m-1)\setminus\tau} \cup \{b\} \cup C' \cup D)^{-1} \\
&= \sum_{\substack{C' \subseteq C \\ |C'|=r}} \sum_{\tau \subseteq m-1} (-1)^{|\tau|} P(\overline{A}_\tau \cup \{a\} \cup \overline{B}_{(m-1)\setminus\tau} \cup C' \cup D) \\
&\quad \times \prod_{\substack{z \in \overline{A}_{(m-1)\setminus\tau} \cup \overline{B}_\tau \cup \{b\} \\ \cup (C \setminus C') \cup D}} \det(z, \overline{A}_\tau \cup \{a\} \cup \overline{B}_{(m-1)\setminus\tau} \cup C' \cup D)^{-1}.
\end{aligned}$$

Rearranging this to one side proves the induction. □

Applying the above corollary to the condition $|\mathcal{A}| = q+2$, i.e. $t = n-3$ leads to

Corollary 8. When $|\mathcal{A}| = q+2$ and $m = n-1-r \geq n-p$ we have

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup E} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}.$$

Proof. Since $|C \setminus C'| = t+2-m-r = (n-1)-(n-1-r)-r = 0$ the corresponding factors vanish in the product of the last corollary. For the same reason $D = \emptyset$. □

Corollary 9 (the case $n \leq 2p-2$). Any arc $\mathcal{A}$ in $\mathrm{P}\mathbb{F}_q^n$ with $n \leq 2p-2$ satisfies the bound $|\mathcal{A}| \leq q+1$.

Proof. We may assume that $n > p$ by the previous work. Apply the previous corollary for $r = p-1$, then $|E| = p-2$, $|C| = p-1$ and $|A| = |B| = n-p$. Write E as $E = F \cup G$ where

$|F| = 2p - 2 - n$ (here we use the assumption) and $|G| = n - p > 0$. Rewriting the equation of in the last corollary delivers

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}.$$

We now aim to prove the following equation for $0 \leq s \leq n - p$ for which the above is the base of induction (inducting on $s \coloneqq |D| = |F| - (2p - 2 - n)$)

$$0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{w \in D} \det(w, A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}.$$

for $D \subseteq A$ an s-element set (which is possible since $|A| = n - p \geq s$).

For the induction step we pick $d \in D$ and $g \in G$, $f \in F$, assume the hypothesis to be proven for $s - 1$ and apply this to our sets A, B, C, $D \setminus \{d\}$, $F \setminus \{f\}$, $G \setminus \{g\} \cup \{f\}$

$$\begin{aligned} 0 = \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{w \in D\setminus\{d\}} \det(w, A_\tau \cup B_{m\setminus\tau} \cup C) \\ \times \det(g, A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}. \end{aligned}$$

Now, we use in the interpolation formula for the determinants as given in Lemma 6.2 (p. 28). Multiplying the above by

$$\operatorname{sgn}(g, \{d\} \cup (G \cup \{f\}) \setminus \{g\} \cup C) \det(\{d\} \cup (G \cup \{f\}) \setminus \{g\} \cup C)$$

and summing over $g \in G \cup \{f\}$ gives (by interpolation of determinants)

$$\begin{aligned} 0 = -\operatorname{sgn}(d, G \cup \{f\} \cup C) \det(G \cup \{f\} \cup C) \sum_{\tau \subseteq m} (-1)^{|\tau|} P(A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{w \in D\setminus\{d\}} \det(w, A_\tau \cup B_{m\setminus\tau} \cup C) \\ \times \det(d, A_\tau \cup B_{m\setminus\tau} \cup C) \prod_{z \in A_{m\setminus\tau} \cup B_\tau \cup F \cup G} \det(z, A_\tau \cup B_{m\setminus\tau} \cup C)^{-1}, \end{aligned}$$

where we can omit the sgn and det at the beginning to see that we are done with the induction step. Of course, the above argument does only work for $s = |D| \leq |A| = n - p$. Applying the formula which we have just proven for $s = n - p$ (i.e. $D = A$) we get

$$P(B \cup C) \prod_{w \in A} \det(w, B \cup C) \prod_{z \in A \cup F \cup G} \det(z, B \cup C)^{-1} = 0$$

since all terms where $\tau \neq \emptyset$ vanish. This clearly is a contradiction. Lastly, we have to verify that $A \cup B \cup C \cup F \cup G$ is not bigger than $q + 2$. Adding the cardinalities leads to

$$|A \cup B \cup C \cup F \cup G| = 2(n - p) + (p - 1) + (p - 2) + (n - p) = 3n - 3 - p.$$

But this is no restriction since $p \leq \sqrt{q}$ and thus $n \leq 2\sqrt{q} - 2$ so $3n - 3 - p < 3n - 3 \leq 6\sqrt{q} - 9 \leq q$. □

Remark 19. The author's proposal is to call the above the A–G lemma.

7 A connection to the KNESER graphs KG$(2n-3, n-2)$

In this section we want to give an alternative proof of the MDS main conjecture for $n \leq p$ using essentially the same means as before and some known facts about the eigenvalues of KNESER graphs.

We recall the interpolation lemma for the tangent polynomials which states that for disjoint subsets $A, B \subseteq \mathcal{A}$ ($|A| = t+2$, $|B| = n-2$ and w.l.o.g. $t+n < |\mathcal{A}|$ using the dual arc if necessary) it holds

$$\sum_{a \in A} P(\{a\} \cup B) \prod_{z \in A \setminus \{a\}} \det(z, \{a\} \cup B)^{-1} = 0 \tag{2}$$

(this is Lemma 6.3 (p. 29) for $r = 1$). Now, we define the interpolation terms as

$$I(C, D) := P(C) \prod_{d \in D} \det(d, C)^{-1}$$

where $C, D \subseteq \mathcal{A}$, $|C| = n-1$, $|D| = t+1$. Reconsidering equation (2) for all possible choices of the sets A and B one obtains a linear system of

$$\binom{|\mathcal{A}|}{t+2, n-2, |\mathcal{A}|-n-t}$$

equations in

$$\binom{|\mathcal{A}|}{t+1, n-1, |\mathcal{A}|-n-t}$$

variables, namely

$$\sum_{a \in A} I(A \setminus \{a\}, \{a\} \cup B) = 0 \text{ for } A \in \binom{\mathcal{A}}{t+2},\ B \in \binom{\mathcal{A}}{n-2},\ A \cap B = \emptyset. \tag{3}$$

Moreover, this system decomposes into $\binom{|\mathcal{A}|}{n+t}$ independent components on which $A \cup B = E$ where $E \in \binom{\mathcal{A}}{t+n}$ is constant.

Note that for the critical case $t = n-3$ there are the same number of variables as equations. We will show that in this case each such component can be interpreted as the adjacency matrix of the KNESER graph KG$(2n-3, n-2)$ and deduce that it is regular when interpreted as a matrix in $\mathbb{Z}/p\mathbb{Z}$ where $n \leq p$ using a fact about the eigenvalues of KNESER graphs.

Lemma 7.1. *Assume $t = n-3$ (i.e. $|\mathcal{A}| = q+2$). Let $E \in \binom{\mathcal{A}}{t+n}$. Then the component of the linear system (3) on which $A \cup B = E$ is the adjacency matrix of the graph* KG$(2n-3, n-2)$.

Proof. Let $x_D := I(E \setminus D, D)$. For each $(n-2)$-set $C \subseteq E$ there is an equation

$$\sum_{D : C \cap D = \emptyset} x_D = 0$$

and this is clearly the system $Ax = 0$ where $A = (a_{CD})$ is the adjacency matrix of $\mathrm{KG}(2n-3, n-2)$ with

$$a_{CD} = \begin{cases} 1 & : C \cap D = \emptyset \\ 0 & : \text{otherwise} \end{cases}.$$

and $x = (x_D)$. □

For $n \leq p$ one derives easily a contradiction from this using a well-known fact about the eigenvalues of KNESER graphs.

Lemma 7.2 (graph spectrum of KNESER graphs). *Let $2k \leq n$. Then the eigenvalues in $\mathbb{Q}$ of the adjacency matrix of the* KNESER *graph $\mathrm{KG}(n,k)$ are*

$$\lambda_j := (-1)^j \binom{n-k-j}{k-j}$$

for $j = 0, \ldots, k$ where λ_j has geometric and algebraic multiplicity $\binom{n}{j} - \binom{n}{j-1}$.

We present the proof given in [7].

Proof. Set

$$V_j := \bigoplus_{\substack{A \subseteq n \\ |A|=j}} \mathbb{Q}A$$

for $j = 0, \ldots, n$. Moreover, define linear mappings $\phi_{ij}^l : V_j \to V_i$ by

$$\phi_{ij}^l(B) = \sum_{\substack{A \subseteq n \\ |A \cap B| = l, |A| = i}} A$$

and linear continuation. For these we may compute that

$$\begin{aligned}
\phi_{ij}^l \circ \phi_{jk}^m(C) &= \sum_{\substack{B \subseteq n \\ |B \cap C| = m, |B| = j}} \sum_{\substack{A \subseteq n \\ |A \cap B| = l, |A| = i}} A \\
&= \sum_{\substack{A \subseteq n \\ |A| = i}} \left| \{ B \subseteq n : |B| = j \wedge |A \cap B| = l \wedge |B \cap C| = m \} \right| A \\
&= \sum_{\nu \in \mathbb{N}} \sum_{\substack{A \subseteq n \\ |A| = i, |A \cap C| = \nu}} \left(\sum_{\mu=0}^{\nu} \binom{i-\nu}{l-\mu} \binom{k-\nu}{m-\mu} \binom{\nu}{\mu} \binom{n-i-k+\nu}{j-l-m+\mu} \right) A \\
&= \sum_{\nu \in \mathbb{N}} \left(\sum_{\mu=0}^{\nu} \binom{i-\nu}{l-\mu} \binom{k-\nu}{m-\mu} \binom{\nu}{\mu} \binom{n-i-k+\nu}{j-l-m+\mu} \right) \phi_{ik}^{\nu}(C)
\end{aligned}$$

where we rearrange the sets A ordered by the size ν of $|A \cap C|$ and then count the sets B which intersect with A and C in the right amount (here μ is $|A \cap B \cap C|$). This implies the identities

$$\phi_{ij}^j \circ \phi_{jk}^k = \binom{i-k}{j-k} \phi_{ik}^k,$$

$$\phi_{ij}^i \circ \phi_{jk}^j = \binom{k-i}{j-i} \phi_{ik}^i,$$

and

$$\phi_{ij}^0 \circ \phi_{jk}^k = \binom{n-i-k}{j-k} \phi_{ik}^0. \tag{4}$$

From the first identity we deduce that $\operatorname{im}(\phi_{ik}^k) \subseteq \operatorname{im}(\phi_{ij}^j)$ for $k \leq j \leq i$. Similarly, from the third we get $\operatorname{im} \phi_{ik}^0 \subseteq \operatorname{im} \phi_{ij}^0$ for $k \leq j \leq n-i$. Moreover, we need the identities

$$\phi_{ij}^j = \sum_{k=0}^{j} (-1)^k \phi_{ik}^0 \circ \phi_{kj}^k. \tag{5}$$

and

$$\phi_{ij}^0 = \sum_{k=0}^{j} (-1)^k \phi_{ik}^k \circ \phi_{kj}^k. \tag{6}$$

The equation (6) follows from (5) by composing with the linearization of the duality map $A \mapsto n \setminus A$ from the left and (5) can be shown by

$$\begin{aligned}\left(\sum_{k=0}^{j} (-1)^k \phi_{ik}^0 \circ \phi_{kj}^k\right)(C) &= \sum_{k=0}^{j} \sum_{\substack{A \subseteq n \\ |A|=i}} (-1)^k \left|\{B \subseteq n : |B| = k \wedge B \subseteq C \setminus A\}\right| A \\ &= \sum_{\substack{A \subseteq n \\ |A|=i}} \delta_{\emptyset, C \setminus A} A = \phi_{ij}^j(C).\end{aligned}$$

Now (5) implies $\operatorname{im} \phi_{ij}^j \subseteq \bigcup_{k=0}^j \operatorname{im} \phi_{ik}^0 = \operatorname{im} \phi_{ij}^0$ $(j \leq n-i)$ and (6) implies $\operatorname{im} \phi_{ij}^0 \subseteq \bigcup_{k=0}^j \operatorname{im} \phi_{ik}^k = \operatorname{im} \phi_{ij}^j$ $(j \leq i)$ such that $\operatorname{im} \phi_{ij}^0 = \operatorname{im} \phi_{ij}^j$ $(j \leq i \leq n-j)$.

We shall prove that ϕ_{ij}^j is injective if $j \leq i \leq n-j$ which can be done by applying the 'dual' equation of (5)

$$\begin{aligned}\mathrm{id} = \phi_{jj}^j &\overset{(5)}{=} \sum_{k=0}^{j} (-1)^k \phi_{jk}^k \circ \phi_{kj}^0 \\ &\overset{(4)}{=} \left(\sum_{k=0}^{j} \frac{(-1)^k}{\binom{n-j-k}{i-j}} \phi_{jk}^k \circ \phi_{ki}^0\right) \circ \phi_{ij}^j.\end{aligned}$$

Thus it is shown that ϕ_{ij}^j is an embedding when $j \leq i \leq n-i$. Let $k \leq \lfloor n/2 \rfloor$, then define for $j = 0, \ldots, k$ the space U_i as the orthogonal complement of $\operatorname{im} \phi_{k,j-1}^{j-1}$ in $\operatorname{im} \phi_{kj}^j$ (we know that $\operatorname{im} \phi_{k-1,j-1}^{j-1} \subseteq \phi_{kj}^j$). We thus have an orthogonal decomposition

$$\bigoplus_{j=0}^{k} U_j = \operatorname{im} \phi_{kk}^k = V_k,$$

which turns out to be the decomposition into eigenspaces U_j of eigenvalue $\lambda_j = (-1)^j \binom{n-k-j}{k-j}$ and dimension $\binom{n}{j} - \binom{n}{j-1}$.

The formula for the dimension of U_j follows from the fact that ϕ_{kj}^j are embeddings. We are left to prove the eigenspace property.

So take $u \in U_j$ and write $u = \phi_{kj}^j(v)$. As $j \leq k \leq n-j$ it holds that $\operatorname{im} \phi_{ki}^i = \operatorname{im} \phi_{ki}^0$ for $i = 0, \ldots, j-1$ and thus we have by definition of U_j

$$0 = (\phi_{ki}^0)^* \circ \phi_{kj}^j(v) = \phi_{ik}^0 \circ \phi_{kj}^j(v) \overset{(4)}{=} \binom{n-i-j}{k-j} \phi_{ij}^0(v)$$

for $i < j$, i.e. $\phi_{ij}^0(v) = 0$ (as $k \geq j$, $n-i-k \geq 0$). But dually to the statement about the images we have $\ker \phi_{ij}^0 = \ker \phi_{ij}^i$, so $\phi_{ij}^i(v) = 0$. Lastly, we have

$$\phi_{kk}^0 \circ \phi_{kj}^j \overset{(4)}{=} \binom{n-k-j}{k-j} \phi_{kj}^0 \overset{(6)}{=} \binom{n-k-j}{k-j} \sum_{i=0}^{j} (-1)^i \phi_{ki}^i \circ \phi_{ij}^i,$$

which gives $\phi_{kk}^0(u) = \binom{n-k-j}{k-j} u$ as desired (ϕ_{kk}^0 is the adjacency operator of $\mathrm{KG}(n,k)$). □

From this we get a direct proof of corollary Corollary 6 (p. 30) as for $n \leq p$ there are no eigenvalues divisible by p and thus the system of equations (3) must be a regular matrix in the case $t = n-3$. Hence it would follow that $I(C, D) = 0$ for all $C, D \subseteq \mathcal{A}$, $|C| = n-1$, $|D| = n-2$ which contradicts the fact that all these expressions must be units in $\mathbb{F}_q$ (by definition).

Remark 20. Actually, we do not need the adjacency matrix of $\mathrm{KG}(2n-3, n-2)$ to be regular in $\mathbb{F}_q$ for a contradiction — we only need that its kernel contains no vector with only non-zero components.

Conclusion

Summing up, we have given an introduction to the MDS main conjecture and related topics in this thesis. It is self-evident, that there are many things which were left untouched and many questions for which we could not give a satisfactory answer (e.g. the completeness of normal rational curves in finite vector spaces; another gap which could not be closed is whether there is a classification of $(q+1)$-arcs when $n \leq 2p-2$). Indeed, there are better results available in the case where $q = p^e$ for $e \geq 3$ stating that any $(q+1)$-arc is complete if $n \leq C\sqrt{q}$ for an

appropriate constant C (which depends e.g. on the characteristic of $\mathbb{F}_q$). However, it would have taken us too far apart to present these in an appropriate manner to the undergraduate reader. The initial intention — to present the proofs of Ball and de Beule such that they can be understood by an undergraduate student — should basically be achieved.

Index

References

[1] Ball, S. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc 14*, 3 (2012), 733–748.

[2] Ball, S., Blokhuis, A., and Mazzocca, F. Maximal arcs in desarguesian planes of odd order do not exist. *Combinatorica 17*, 1 (1997), 31–41.

[3] Ball, S., and De Beule, J. On sets of vectors of a finite vector space in which every subset of basis size is a basis ii. *Designs, Codes and Cryptography 65*, 1-2 (2012), 5–14.

[4] Beutelspacher, A. *Handbook of Incidence Geometry.* p. 120.

[5] Caullery, F., and Schmidt, K.-U. On the classification of hyperovals. *arXiv preprint arXiv:1403.2880* (2014).

[6] Orlik, P., and Terao, H. *Arrangements of hyperplanes*, vol. 300. Springer, 1992.

[7] Wilson, R. Algebraic techniques in extremal combinatorics, graph theory, and finite geometry, 2011. `http://www.math.caltech.edu/~2011-12/2term/ma192b/kneser-evals.pdf`.

[8] Zaslavsky, T. Facing up to arrangements: face-count formulas for partitions of space by hyperplanes. *Memoirs of the American Mathematical Society 1*, 154 (1975).